Security Measures

Overview

Both Storytailor (our web platform) and Story Intelligence™ (our future AI engine) use the same comprehensive security measures to protect children's data and ensure COPPA compliance. This document describes our security practices and data protection measures that apply to both products.

Encryption

Encryption at Rest

Database Encryption: - All data stored in encrypted databases - Database-level encryption enabled - Encryption keys managed securely - Data cannot be read without proper decryption keys

Storage Encryption: - All file storage encrypted - Asset storage (stories, images, audio) encrypted - Encryption keys managed through secure key management

Configuration and Secrets: - All configuration secrets encrypted - API keys and credentials encrypted - Secure key management system used

Encryption in Transit

API Communications: - All API endpoints require HTTPS/TLS - TLS 1.3 used for all API communications - No unencrypted data transmission allowed - Certificate validation enforced

Database Connections: - All database connections use SSL/TLS - Encrypted connections required - Certificate validation enforced

Email Delivery: - All email communications use TLS encryption - Encrypted email delivery to parents - Secure email transmission protocols

Access Control

Row Level Security (RLS)

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

RLS Policy Enforcement: - Policies enforced at database level - Cannot be bypassed by application code - Automatic enforcement on all queries - User-based access control

Authentication

API Authentication: - All API endpoints require authentication - JWT Bearer tokens used for authentication - Token validation on every request - Token expiration and refresh mechanisms

Token Security: - Tokens signed with secure keys - Token expiration enforced - Token refresh required periodically - Invalid tokens rejected immediately

Authorization

User Authorization: - User-based access control - Users can only access their own data - Parent-child relationship verification - Service role access restricted to system operations

Parent Authorization: - Parents must verify identity to access child data - Parent-child relationship validated - Parent email verification required - Authorization checked on every request

Data Access Controls

User Data Access

Self-Access: - Users can access their own data - Access limited to user's own stories, characters, and preferences - Cannot access other users' data

Parent Access: - Parents can access their own child's data - Parent-child relationship verified - Access limited to parent's own children - Cannot access other children's data

Service Access

System Operations: - Service role access only for system operations - Limited to necessary operations - All service access logged - Regular review of service access

Administrative Access: - Administrative access restricted - Multi-factor authentication required - All administrative actions logged - Regular access reviews

Audit Logging

Logged Events

Authentication Events: - User login attempts - Authentication successes and failures - Token generation and validation - Session creation and termination

Consent Events: - Consent request creation - Consent verification - Consent revocation - Consent status checks

Data Access Events: - Parent data access requests - Data export requests - Data deletion requests - Data modification events

Safety Events: - Safety incident detection - Parent notifications sent - Crisis intervention triggered - Safety monitoring events

Security Events: - API errors and security violations - Unauthorized access attempts - Authentication failures - Security policy violations

Audit Log Features

Log Contents: - User ID (anonymized for children) - Action type - Resource type and ID - Timestamp - IP address (anonymized for children) - User agent - Additional context

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

Log Security: - Audit logs encrypted - Log access restricted - Log integrity protected - Log tampering detection

Security Monitoring

Continuous Monitoring

Security Monitoring: - Real-time security event monitoring - Automated alerting for security incidents - Regular security reviews - Incident response procedures

Threat Detection: - Unauthorized access attempt detection - Anomaly detection - Security violation detection - Automated response to threats

Regular Security Reviews

Access Reviews: - Regular review of user access - Regular review of service access - Regular review of administrative access - Access revocation when no longer needed

Security Assessments: - Regular security assessments - Vulnerability scanning - Penetration testing (as needed) - Security policy reviews

Incident Response

Security Incident Response

Incident Detection: - Automated security incident detection - Manual incident reporting - Security monitoring alerts - User-reported incidents

Incident Response Process: 1. Incident detection and reporting 2. Incident assessment and classification 3. Containment of incident 4. Investigation and analysis 5. Remediation and recovery 6. Post-incident review and improvement

Notification Requirements: - Parents notified of security incidents affecting their child - Authorities notified if required by law - Incident documentation and reporting - Post-incident security improvements

Data Protection for Children

Enhanced Protections

COPPA-Protected Users: - Enhanced security measures for children under 13 - Stricter access controls - Enhanced audit logging - Additional privacy protections

Data Minimization: - Only necessary data collected - Shorter retention periods - Faster data deletion - Enhanced anonymization

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

Infrastructure Security

Cloud Infrastructure

Infrastructure Security: - Secure cloud infrastructure - Network security controls - Firewall rules and access controls - DDoS protection

Service Security: - Secure service configuration - Regular security updates - Vulnerability patching - Security best practices

Third-Party Security

Service Provider Security: - All third-party services meet security requirements - Data Processing Agreements (DPAs) in place - Security certifications verified - Regular security reviews

Data Sharing: - Minimal data sharing with third parties - Only necessary data shared - Secure data transmission - Third-party security verified

Compliance and Certification

Security Compliance

Compliance Standards: - COPPA compliance - GDPR compliance - Industry security best practices - Regular compliance audits

Security Certifications: - Third-party services maintain security certifications - Regular security assessments - Compliance verification - Ongoing security improvements

Contact Information

Security Inquiries: privacy@storytailor.com
Security Incidents: safety@storytailor.com
Technical Contact: tech@storytailor.com
Mailing Address:
Storytailor Inc.
7131 w 135th, #1074
Overland Park, KS 66223

Response Time: Security incidents responded to immediately. All security inquiries responded to within 30 days.

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