# Talenpal Children’s Privacy Agreement

**Effective Date:** September 20, 2025  
**Last Updated:** September 20, 2025

**Company:** Talenpal HK Limited  
**Address:** UNIT 903D 9/F CAMERON COMM CTR 458-468 HENNESSY RD CAUSEWAY BAY, Hong Kong  
**Email:** privacy@talenpal.com  
**Data Protection Officer:** dpo@talenpal.com

## 1. Introduction and Scope

Welcome to Talenpal! This Children’s Privacy Agreement (“Agreement”) is specifically designed to protect children under 13 years old who use our mobile application (“App”) and interactive storytelling devices. Talenpal HK Limited (“Talenpal,” “we,” “us,” or “our”) is committed to providing the highest level of privacy protection for our young users.

**Important Notice for Parents and Guardians:** This Agreement governs our collection, use, and protection of your child’s personal information. We strictly comply with the Children’s Online Privacy Protection Act (COPPA), state biometric privacy laws, and other applicable privacy regulations. Your child’s privacy and safety are our top priorities.

Scope of Application: This Agreement applies to: - Children under 13 years old using Talenpal App - All personal information collected from or about children - All interactions with our AI voice features and storytelling services - Data collected through our physical storytelling devices

## 2. Definition of Children’s Personal Information

Under this Agreement and applicable laws, “Children’s Personal Information” includes any information that can be used to identify, contact, or locate a child, including but not limited to:

**Basic Identity Information:** - Child’s first name or nickname - Any combination of last name with other identifiers - Home address or geolocation information - Social security numbers or other government identifiers

**Contact Information:** - Email addresses created for or by the child - Phone numbers associated with the child - Any instant messaging identifiers

**Digital Identifiers:** - Persistent identifiers such as customer numbers stored in cookies - IP addresses when connected to personal information - Device identifiers that can track a user over time and across websites

**Biometric Information:** - Voice recordings and voice prints - Photos or videos containing the child’s image - Any biometric identifiers derived from voice or image data

**Behavioral Data:** - Website and app usage patterns - Preferences and interests - Interaction history with our AI characters

## 3. Types of Children’s Information We Collect

### 3.1 Information Directly Provided

* **Child’s First Name:** Used for personalization in storytelling and AI interactions
* **Family Context Information:** Basic information about family activities, pets, or interests to enhance storytelling (collected only with explicit parental consent for each category)
* **Preferences:** Story categories, favorite characters, or content preferences

### 3.2 Voice and Audio Data

* **Voice Commands:** Audio recordings when your child interacts with our AI voice features
* **Conversational Audio:** Recordings during interactive storytelling sessions
* **Technical Voice Data:** Acoustic features needed for speech recognition (not unique voice prints)

### 3.3 Automatically Collected Information

* **Device Information:** Device type, operating system version, app version
* **Usage Analytics:** How the App is used, session duration, feature utilization (anonymized)
* **Technical Support Data:** Error logs and diagnostic information (without personal identifiers)

### 3.4 Information We Do NOT Collect

We do not collect: - Precise geolocation information - Social security numbers or government IDs - Credit card or payment information directly from children - Information from social media profiles - Data from third-party educational or gaming platforms without explicit consent

## 4. Purpose and Methods of Information Collection

### 4.1 Collection Purposes

We collect children’s personal information solely for these limited purposes:

**Core Service Delivery:** - Providing personalized storytelling experiences - Enabling voice-controlled interactions with AI characters - Synchronizing content between app and physical devices - Maintaining user preferences and progress

**Safety and Security:** - Monitoring for inappropriate content or behavior - Protecting against technical issues or service disruptions - Preventing unauthorized access to accounts

**Service Improvement:** - Improving AI voice recognition accuracy (using anonymized data only) - Enhancing storytelling algorithms - Fixing bugs and technical issues

### 4.2 Collection Methods

Information is collected through: - Direct input during app setup and usage - Voice recordings during interactive sessions - Automatic collection through app functionality - Parent-provided information during account setup

### 4.3 Data Minimization Principle

We adhere strictly to data minimization, collecting only the minimum information necessary to provide our core services. We do not collect information for: - Marketing or advertising purposes - Creating detailed behavioral profiles - Commercial use beyond our core services - Third-party monetization

## 5. Parental Consent Mechanism

### 5.1 Verifiable Parental Consent Requirement

Before collecting any personal information from your child, we obtain Verifiable Parental Consent (VPC) as required by COPPA.

**Our Simplified Consent Method:** We use **SMS Verification** as our primary method for verifiable parental consent:

1. **Phone Number Verification:** Parents provide their mobile phone number
2. **SMS Confirmation:** We send a unique verification code via SMS
3. **Code Verification:** Parents enter the code to confirm their identity
4. **Consent Confirmation:** Parents explicitly agree to data collection for their child

**Why We Choose SMS Verification:** - More accessible than credit card verification - Simpler than government ID verification - More convenient than video conferencing - Provides adequate verification while maintaining ease of use

### 5.2 Consent Scope and Granularity

Our consent process covers: - **Initial Setup:** Basic information needed for core functionality - **Voice Features:** Separate consent for voice recording and AI interaction features - **Enhanced Personalization:** Additional consent for collecting family context information - **Feature-Specific Consent:** Separate approval for new features that require additional data

### 5.3 Consent Documentation

We maintain detailed records of: - Date and time of consent - Specific information categories consented to - Parent contact information - Consent method used - Any subsequent consent modifications

## 6. Use and Sharing of Information

### 6.1 Information Use

Children’s personal information is used exclusively for:

**Primary Uses:** - Customizing storytelling content with child’s name and interests - Processing voice commands for interactive features - Matching user profiles with device content - Providing technical support when requested

**Secondary Uses (with specific consent):** - Improving AI voice recognition (using anonymized voice data) - Enhancing content recommendations - Conducting safety monitoring for inappropriate content

### 6.2 Information Sharing Limitations

We strictly limit information sharing and do not: - Sell or rent children’s personal information - Share information for advertising purposes - Create marketing profiles based on children’s data - Allow third-party tracking or behavioral advertising

### 6.3 Permitted Sharing

We may share children’s information only in these limited circumstances:

**Service Providers:** With trusted third parties who help operate our services, including: - Cloud storage providers (AWS with COPPA-compliant contracts) - Technical support providers (access limited to specific support requests) - Analytics providers (using only anonymized, aggregate data)

**Legal Requirements:** - When required by law enforcement with proper legal authority - To protect the immediate safety of a child - To defend our legal rights in litigation

**Corporate Transactions:** - In the event of a merger or acquisition (with equivalent privacy protections)

## 7. Storage and Protection of Children’s Information

### 7.1 Data Security Measures

**Technical Safeguards:** - **Encryption at Rest:** AES-256 encryption for all stored data - **Encryption in Transit:** TLS 1.3 for all data transmission - **Access Controls:** Multi-factor authentication for all staff access - **Network Security:** Firewalls and intrusion detection systems

**Administrative Safeguards:** - **Staff Training:** Regular privacy and security training for all employees - **Background Checks:** Comprehensive screening for personnel with data access - **Access Limitation:** Strict need-to-know basis for data access - **Regular Audits:** Quarterly security assessments and annual third-party audits

**Physical Safeguards:** - **Secure Data Centers:** SOC 2 Type II certified facilities - **Limited Physical Access:** Biometric controls and surveillance - **Equipment Security:** Secure disposal of hardware containing data

### 7.2 Data Storage Locations

* Primary data storage: Secure cloud infrastructure in the United States
* Backup storage: Encrypted backups in geographically separate locations
* International transfer safeguards: Appropriate legal frameworks for any data transfer

### 7.3 Data Breach Response

In the event of a security incident: - Immediate containment and assessment within 24 hours - Parent notification within 72 hours - Detailed incident report including affected information types - Free credit monitoring services if applicable - Implementation of additional security measures

## 8. Parental Rights and Controls

### 8.1 Core Parental Rights

As a parent or guardian, you have the right to:

**Access Rights:** - View all personal information we have collected about your child - Receive a copy of your child’s data in a readable format - Understand how the information is being used

**Control Rights:** - Refuse further collection of your child’s information - Request corrections to inaccurate information - Delete your child’s account and all associated data - Withdraw consent for specific data uses

**Oversight Rights:** - Monitor your child’s app usage and interactions - Set restrictions on features and content - Receive notifications about new data collection

### 8.2 Parental Dashboard

We provide a comprehensive parent dashboard where you can: - View all collected information about your child - Manage privacy settings and consent preferences - Download a copy of your child’s data - Request data deletion - Control access to specific app features - Monitor usage patterns and screen time

### 8.3 Exercising Parental Rights

To exercise your rights:

**Online:** Use the parent dashboard in our app **Email:** Send requests to privacy@talenpal.com **Response Time:** We respond to all requests within 10 business days

## 9. Information Retention and Deletion

### 9.1 Retention Periods

**Active Account Data:** - Child’s name and preferences: Retained while account is active - Usage data: Anonymized after 90 days, retained for service improvement - Voice recordings: Automatically deleted after 30 days - Technical support data: Deleted after issue resolution

**Inactive Account Data:** - Account review after 12 months of inactivity - 30-day notice before automatic deletion - Complete data removal if no response received

### 9.2 Automatic Deletion Processes

* **Voice Data:** Automatic deletion after 30 days unless specifically needed for technical support
* **Session Data:** Real-time data cleared after each session
* **Cache Data:** Temporary data cleared every 24 hours
* **Analytics Data:** Personal identifiers removed within 90 days

### 9.3 Deletion Upon Request

When you request data deletion: 1. **Identity Verification:** Confirm your identity as the parent/guardian 2. **Scope Confirmation:** Clarify which data should be deleted 3. **Processing Time:** Complete deletion within 30 days 4. **Confirmation:** Email confirmation of deletion completion 5. **Backup Removal:** Data removed from all systems including backups

### 9.4 Retention Exceptions

We may retain anonymized, non-personal data for: - Service improvement and analytics - Safety and security monitoring - Legal compliance requirements

## 10. Third-Party Services

### 10.1 Approved Third-Party Partners

We work only with carefully vetted third-party service providers who: - Sign COPPA-compliant data processing agreements - Undergo regular security audits - Agree to use data only for specified purposes - Implement equivalent privacy protections

**Current Third-Party Services:** - **Cloud Infrastructure:** AWS (Amazon Web Services) with COPPA Business Associate Agreement - **Analytics:** Custom analytics solution with data anonymization

### 10.2 Third-Party Limitations

Our third-party partners are contractually prohibited from: - Using children’s data for their own purposes - Sharing data with other parties - Creating profiles for advertising - Retaining data beyond service requirements

### 10.3 Third-Party Monitoring

We regularly monitor third-party compliance through: - Quarterly compliance reports - Annual security assessments - Real-time access monitoring - Contract compliance audits

## 11. Data Security Measures

### 11.1 Comprehensive Security Framework

**Data Encryption:** - **AES-256 Encryption:** Industry-standard encryption for all stored data - **TLS 1.3 Protocol:** Secure transmission for all data in transit - **Key Management:** Secure encryption key storage and rotation - **End-to-End Protection:** Data protected throughout its lifecycle

**Access Security:** - **Multi-Factor Authentication:** Required for all staff access - **Role-Based Access:** Strict permissions based on job requirements - **Access Logging:** Complete audit trail of all data access - **Regular Access Reviews:** Quarterly review and update of access permissions

**Infrastructure Security:** - **SOC 2 Compliance:** Annual third-party security audits - **Penetration Testing:** Semi-annual security testing - **Vulnerability Management:** Regular scanning and patch management - **Incident Response:** 24/7 security monitoring and response team

### 11.2 Voice Data Security

Special protections for voice recordings: - **Real-Time Encryption:** Voice data encrypted during recording - **Secure Processing:** Voice analysis performed in secure, isolated environments - **Limited Retention:** Automatic deletion after 30 days - **No Voice Prints:** We do not create permanent voice identification profiles

### 11.3 Security Training and Awareness

* **Employee Training:** Mandatory privacy and security training for all staff
* **Regular Updates:** Quarterly training updates on new threats and procedures
* **Incident Simulation:** Annual security incident response drills
* **Privacy Champions:** Designated privacy officers in each department

## 12. International Data Transfers

### 12.1 Transfer Framework

As a Hong Kong-based company serving U.S. customers: - **Primary Storage:** Data stored primarily in U.S.-based secure facilities - **Limited Transfers:** Data may be transferred to Hong Kong for technical support - **Legal Safeguards:** All transfers protected by appropriate legal mechanisms - **Parental Notification:** Parents informed of international processing during consent

### 12.2 Transfer Protections

* **Contractual Safeguards:** Standard contractual clauses for data protection
* **Adequacy Assessments:** Regular review of transfer destination privacy laws
* **Additional Security:** Enhanced security measures for international transfers
* **Data Minimization:** Only necessary data transferred internationally

### 12.3 Your Rights Regarding Transfers

* **Transparency:** Full disclosure of where data is processed
* **Objection Rights:** Ability to object to certain international transfers
* **Local Access:** Ability to access and control data regardless of location

## 13. Policy Updates

### 13.1 Update Process

We may update this Privacy Agreement to: - Reflect changes in our services - Comply with new legal requirements - Implement enhanced privacy protections - Address user feedback and concerns

### 13.2 Notification Procedures

When we make changes: - **30-Day Notice:** Email notification to parents 30 days before changes take effect - **Change Summary:** Clear explanation of what has changed and why - **Consent Requirements:** New consent obtained if required by law - **Continued Access:** Ability to withdraw consent if you disagree with changes

### 13.3 Material Changes

For significant changes affecting data collection or use: - **Explicit Consent:** New verifiable parental consent required - **Opt-Out Options:** Ability to continue using service with previous privacy settings - **Account Deletion:** Option to delete account if changes are unacceptable

## 14. Contact Us

### 14.1 Privacy Team Contact Information

**General Privacy Inquiries:** - **Email:** privacy@talenpal.com - **Hours:** Monday-Friday, 9 AM - 6 PM EST - **Response Time:** 24 hours for urgent matters, 48 hours for general inquiries

**Data Protection Officer:** - **Email:** dpo@talenpal.com - **Address:** Talenpal HK Limited, [Company Address], Hong Kong

### 14.2 Exercising Your Rights

To access, correct, or delete your child’s information:

**Online:** Parent Dashboard in the Talenpal App **Email:** privacy@talenpal.com with subject “Parental Rights Request” **Mail:** Talenpal HK Limited, Privacy Team, [Company Address], Hong Kong

**Required Information for Requests:** - Parent’s full name and contact information - Child’s name and account information - Specific request (access, correction, deletion) - Verification information (account details or SMS verification)

### 14.3 Complaints and Concerns

If you have concerns about our privacy practices:

**Internal Resolution:** 1. Contact our Privacy Team first 2. Escalate to Data Protection Officer if needed 3. Request supervisory review if unsatisfied

**External Resolution:** - **FTC Complaint:** File complaint with Federal Trade Commission - **State Authorities:** Contact your state’s consumer protection office - **Legal Consultation:** Seek advice from privacy law attorneys

### 14.4 Emergency Contact

For urgent privacy or safety concerns: **Emergency Email:** emergency@talenpal.com - **Response Time:** Immediate response for child safety issues

## Compliance Certifications

**This Children’s Privacy Agreement complies with:** - Children’s Online Privacy Protection Act (COPPA) - California Consumer Privacy Act (CCPA) for minors - Illinois Biometric Information Privacy Act (BIPA) - Texas Capture or Use of Biometric Identifier Act - Washington State Biometric Privacy Law - Federal Trade Commission (FTC) Guidelines for Children’s Privacy

**Regular Compliance Reviews:** - Quarterly internal privacy assessments - Annual third-party privacy audits - Ongoing monitoring of regulatory changes - Regular updates to maintain compliance

**Document Information:** - **Version:** 1.0 - **Legal Review Date:** September 20, 2025 - **Next Review Date:** September 20, 2025 - **Document Classification:** Public - **Language:** English - **Jurisdiction:** United States, with Hong Kong entity operations

**For Parents:** This Agreement is designed to give you complete control over your child’s personal information while allowing them to enjoy safe, personalized storytelling experiences. If you have any questions about this Agreement or your rights as a parent, please contact us at privacy@talenpal.com. We are committed to protecting your child’s privacy and providing transparent, trustworthy service.

**© 2025 Talenpal HK Limited. All rights reserved.**