# Talenpal Content Creation User Agreement

**Last Updated: September 20, 2025**

## 1. Agreement Overview

Welcome to the Talenpal content creation platform (hereinafter referred to as “the Platform” or “we”). This Agreement constitutes a legally binding agreement between you and Talenpal HK Limited regarding the use of content creation services.

### 1.1 Scope of Application

This Agreement applies to all content creation features provided by the Platform, including but not limited to: - User-generated original content creation (stories, text, images, etc.) - Voice cloning technology services - AI-generated content tools - Content publishing and sharing features

### 1.2 Special Declaration

Given that this Platform primarily serves child users (under 13 years of age), we will strictly comply with the highest standards of relevant laws and regulations such as the Children’s Online Privacy Protection Act (COPPA).

## 2. User Eligibility and Parental Consent

### 2.1 Age Restrictions

* Users 13 years and older may independently use Platform services
* Child users under 13 years must obtain verifiable consent from parents or legal guardians to use the service

### 2.2 Parental Consent Requirements (applicable to users under 13)

In accordance with COPPA requirements, we will:

#### 2.2.1 Verifiable Parental Consent Mechanism

Parents must provide consent through any of the following methods: Phone number verification - Credit card or debit card verification (conducting small verification transactions) - Government-issued identification verification - Phone or video call confirmation - Signing and submitting written consent forms - Knowledge-based identity verification questions

#### 2.2.2 Withdrawal of Consent

Parents have the right to withdraw consent at any time, requiring: - Cessation of collection of children’s personal information - Deletion of already collected children’s personal information - Termination of services provided to children

### 2.3 Parental Supervision Obligations

Parents or guardians shall: - Supervise all activities of children on the Platform - Regularly review content created by children - Ensure children comply with Platform community guidelines - Bear legal responsibility for children’s behavior on the Platform

## 3. Content Creation and Intellectual Property

### 3.1 User Content Ownership

#### 3.1.1 Basic Principles

* Users retain complete intellectual property rights to their original content
* Child creators enjoy copyright to their works regardless of age limitations
* The Platform does not claim ownership of user-generated original content

#### 3.1.2 Special Provisions for Children’s Creative Content

For content created by children under 13: - Intellectual property rights belong to the child - Authorization decisions regarding commercial use must be made by parents or guardians on behalf of the child - The Platform will assist in establishing revenue protection mechanisms for children’s content creation

### 3.2 Platform Usage License

#### 3.2.1 Necessary Authorization Scope

Users agree to grant the Platform the following limited rights: - Display user content on the Platform - Conduct necessary technical processing for service provision (such as format conversion, thumbnail generation) - Distribute and recommend content according to user settings - Analyze content for security review purposes

#### 3.2.2 Authorization Limitations

This authorization does not include: - Using user content for commercial advertising or marketing - Selling or transferring user content to third parties - Making substantial modifications or derivative works of user content

### 3.3 Revenue Sharing (applicable to content generating commercial value)

For child creators who generate commercial revenue through the Platform: - Trust funds will be established in accordance with relevant legal requirements - Ensure legitimate economic rights of child creators - Provide transparent revenue distribution mechanisms

## 4. Voice Cloning Technology Services

### 4.1 Service Description

The Platform provides artificial intelligence-based voice cloning technology, allowing users to: - Create personal voice models - Generate audio content based on voice models - Use voice models in creative works

### 4.2 Voice Rights Protection

#### 4.2.1 Legal Basis

According to the Personality Rights section of the Civil Code and relevant laws: - Individual voices are protected by personality rights, with reference to portrait rights provisions - Unauthorized use of others’ voices for AI cloning constitutes infringement - AI-generated content with identifiable voices must be clearly marked

#### 4.2.2 User Representations and Warranties

Users using voice cloning functions must represent and warrant: - They possess legal rights to the provided voice samples - They do not infringe upon any third party’s voice rights - They will not use cloned voices for fraud, defamation, or other illegal purposes

### 4.3 Clear and Specific Consent Requirements

#### 4.3.1 Obtaining Consent

Before collecting voice data, we will: - Explain the purpose of voice collection in clear and understandable language - Provide detailed explanations of how voice cloning technology works - Clearly inform users of the scope and duration of voice data usage - Explain data storage and sharing policies

#### 4.3.2 Characteristics of Consent

User consent must be: - **Explicit**: Expressed through active actions (such as checking checkboxes) - **Informed**: Made after full understanding of relevant information - **Specific**: Targeted to specific purposes and processing activities - **Revocable**: Users may withdraw consent at any time

### 4.4 Voice Data Protection

#### 4.4.1 Data Security Measures

* Employ industry-leading encryption technology to protect voice data
* Implement strict access control and audit mechanisms
* Regularly conduct security risk assessments and vulnerability fixes

#### 4.4.2 Data Minimization Principle

* Collect only the minimum data necessary to achieve voice cloning functionality
* Do not collect additional voice information unrelated to functionality
* Regularly delete voice data that is no longer needed

### 4.5 Usage Restrictions and Prohibited Activities

#### 4.5.1 Strict Prohibitions

Users must not use voice cloning technology to: - Impersonate others for fraudulent activities - Create false information or misleading content - Engage in harassment, threats, or malicious behavior - Infringe upon others’ privacy or personality rights - Create illegal or non-compliant content

#### 4.5.2 Usage Limitations

* Cloning others’ voices requires explicit authorization
* Generated audio content must be clearly marked as AI-generated
* Voice models must not be used for commercial purposes (unless compliant with relevant legal requirements)

## 5. Deepfake Technology Regulation

### 5.1 Definition and Identification of Deepfakes

Deepfakes refer to audio, video, or image content generated or significantly modified using artificial intelligence technology that: - Appears real but is actually false - Can mislead audiences into believing someone said or did something they never actually said or did

### 5.2 Legal Restrictions on Deepfake Content

#### 5.2.1 Prohibited Deepfake Content

Strictly prohibited from creating or distributing: - Non-consensual pornographic or humiliating deepfake content - False content used for fraud or scam purposes - Misleading content that may affect elections or political processes - False content that infringes upon others’ personality rights or reputation - False information that may cause panic or social unrest

#### 5.2.2 Content Marking Requirements

All content generated or significantly modified using AI technology must: - Display “AI-generated” or “AI-modified” labels in prominent positions - Provide authenticity descriptions of the content - Technically embed digital watermarks for traceability

### 5.3 Preventive Measures

#### 5.3.1 Technical Prevention

* Deploy deepfake detection technology
* Implement content traceability and verification mechanisms
* Establish automatic identification and warning systems

#### 5.3.2 User Education

* Provide deepfake identification education
* Promote awareness of relevant legal risks and consequences
* Establish responsible use guidelines

## 6. Content Moderation and Security Mechanisms

### 6.1 Layered Moderation System

#### 6.1.1 Automated Pre-screening

* AI technology for preliminary content screening
* Automatic identification of obviously violating content
* Flag suspicious content for human review

#### 6.1.2 Human Review

* Professional review teams handle complex cases
* Special review standards for children’s content
* Multiple reviews to ensure decision accuracy

### 6.2 Special Protection for Children’s Content

#### 6.2.1 Stricter Review Standards

Apply the strictest standards for content involving children: - Zero tolerance for harmful or inappropriate content - Prioritize protection of children’s safety and privacy - Proactively identify and remove risky content

#### 6.2.2 Safety Features

* Enable highest level privacy settings by default
* Restrict interaction features for children’s accounts
* Disable potentially risky features (such as location sharing)

### 6.3 Reporting and Appeal Mechanisms

#### 6.3.1 Reporting Channels

Provide multiple convenient reporting methods: - Built-in report buttons - Dedicated reporting email - Customer service hotline - Online reporting forms

#### 6.3.2 Appeal Process

For content moderation decisions: - Provide clear appeal channels - Process appeal requests promptly - Fair and transparent review procedures

### 6.4 Community Guidelines

#### 6.4.1 Prohibited Content

* Violent, pornographic, or other content inappropriate for children
* Hate speech or discriminatory content
* False information or misleading content
* Content that infringes upon others’ rights
* Illegal or non-compliant content

#### 6.4.2 Behavioral Standards

* Respect others and communicate kindly
* Protect personal privacy information
* Comply with intellectual property regulations
* Do not engage in bullying or harassment

## 7. Personal Information Protection

### 7.1 Definition of Personal Information (COPPA Standards)

According to COPPA, personal information includes: - Basic identity information such as name, address, phone number - Online contact information such as email, instant messaging IDs - Screen names or usernames (when they have contact functionality) - Persistent identifiers such as IP addresses, device IDs - Photos, videos, audio containing children’s images or voices - Geographic location information - Other information associated with the above information

### 7.2 Information Collection Principles

#### 7.2.1 Minimization Principle

* Collect only the minimum information necessary to provide services
* Do not require additional information as a condition for participation in activities
* Regularly evaluate and reduce data collection scope

#### 7.2.2 Purpose Limitation

* Clearly inform users of specific purposes for information collection
* Do not use information for purposes other than those disclosed
* Obtain separate authorization for additional uses

### 7.3 Data Security Safeguards

#### 7.3.1 Technical Measures

* Data transmission encryption (TLS/SSL)
* Storage data encryption protection
* Access control and identity authentication
* Regular security audits and vulnerability fixes

#### 7.3.2 Administrative Measures

* Establish data security management systems
* Employee data protection training
* Third-party data processing compliance requirements
* Data breach emergency response mechanisms

### 7.4 Data Retention and Deletion

#### 7.4.1 Retention Period

* Retain data only for the period necessary to achieve collection purposes
* Establish clear data retention schedules
* Automatic deletion mechanisms for expired data

#### 7.4.2 Deletion Rights

Users (parents representing children) have the right to request: - Review of collected personal information - Deletion of personal information - Cessation of further collection or use - Withdrawal of consent

## 8. Third-Party Services and Compliance

### 8.1 Third-Party Service Integration

The Platform may integrate the following third-party services: - Analytics and statistics tools - Content delivery networks - Payment processing services - Customer service tools

### 8.2 Third-Party Compliance Requirements

#### 8.2.1 Due Diligence

* Evaluate third parties’ data processing practices
* Confirm their COPPA compliance capabilities
* Review their privacy policies and security measures

#### 8.2.2 Contractual Obligations

Contracts signed with third parties must include: - COPPA compliance obligations - Data protection requirements - Usage restriction clauses - Data deletion obligations

### 8.3 “Support for Internal Operations” Exception

For third-party services used solely to support Platform internal operations: - Crash reporting and performance analysis - Network communication support - Security monitoring - Function maintenance

These services do not require separate parental consent but must be described in the privacy policy.

## 9. Platform Responsibilities and Disclaimers

### 9.1 Platform Obligations

#### 9.1.1 Content Moderation Obligations

* Establish and maintain effective content moderation mechanisms
* Promptly handle violating content and reports
* Continuously improve moderation technology and processes

#### 9.1.2 User Protection Obligations

* Protect users, especially child users’ safety
* Maintain a healthy community environment on the Platform
* Provide safety education and guidance

#### 9.1.3 Legal Compliance Obligations

* Comply with relevant laws and regulations
* Cooperate with law enforcement investigations
* Promptly update compliance policies

### 9.2 Platform Disclaimers

#### 9.2.1 User Behavior Disclaimers

The Platform is not responsible for the following behaviors: - User violations of this Agreement - User infringement of third-party rights - Illegal or non-compliant content uploaded by users - Disputes and conflicts between users

#### 9.2.2 Technical Limitation Disclaimers

* Network service interruptions or delays
* Temporary unavailability due to system maintenance
* Service impacts caused by force majeure factors
* Third-party service failures

#### 9.2.3 Liability Limitations

To the maximum extent permitted by law: - Limit liability for indirect losses and consequential damages - Set upper limits on compensation liability - Exclude liability for special damages

### 9.3 Intellectual Property Protection

#### 9.3.1 Infringement Notice Procedures

Establish DMCA-like notice-and-takedown mechanisms: - Rights holders may submit infringement notices - Platform promptly handles infringing content - Accused users may submit counter-notices

#### 9.3.2 Repeat Infringement Handling

* Maintain user infringement records
* Take restrictive measures against repeat infringers
* Terminate services for serious cases

## 10. Dispute Resolution

### 10.1 Dispute Resolution Methods

#### 10.1.1 Negotiated Settlement

* Encourage resolution of disputes through friendly negotiation
* Provide customer service channels to assist communication
* Establish internal mediation mechanisms

#### 10.1.2 Legal Remedies

If negotiation fails to resolve disputes: - May file lawsuits in courts with jurisdiction - Follow applicable legal procedures - Respect judicial decisions

### 10.2 Applicable Law

#### 10.2.1 Legal Application

The interpretation and execution of this Agreement apply: - Laws of the People’s Republic of China (Chinese users) - United States federal and state laws (US users) - Relevant laws and regulations of users’ jurisdictions

#### 10.2.2 Jurisdiction

* Disputes arising from this Agreement shall be handled by courts with jurisdiction
* Respect judicial jurisdiction provisions of various regions

## 11. Agreement Updates and Notifications

### 11.1 Agreement Modifications

#### 11.1.1 Right to Modify

The Platform reserves the right to modify this Agreement, but must: - Notify users 30 days in advance - Display modifications prominently - Explain reasons for and impacts of modifications

#### 11.1.2 User Choices

After Agreement modifications: - Continued use constitutes acceptance of modifications - Non-acceptance of modifications may result in termination of use - For child users, renewed parental consent is required

### 11.2 Notification Methods

Important notices will be sent through the following methods: - In-platform message push notifications - Email to registered email addresses - Platform announcement board posts - In-app pop-up reminders

## 12. Special Provisions

### 12.1 Protection of Child Creator Rights

#### 12.1.1 Economic Rights

For children who generate revenue through content creation: - Establish dedicated revenue management mechanisms - Ensure compliance with local labor protection laws - Assist in establishing education funds or trust funds

#### 12.1.2 Time Limitations

* Recommend limiting children’s daily creation time
* Provide time management tools
* Encourage balance between learning and creation

### 12.2 Emergency Situation Handling

#### 12.2.1 Emergency Deletion

Content may be immediately deleted in the following situations: - Emergency situations involving child safety - Obviously illegal criminal content - Serious infringement of others’ rights - Content that may cause significant social impact

#### 12.2.2 Law Enforcement Assistance

When required by law: - Cooperate with law enforcement investigations - Provide necessary user information - Preserve relevant evidence materials

### 12.3 Accessible Access

#### 12.3.1 Technical Support

* Support assistive technologies such as screen readers
* Provide multiple interaction methods
* Ensure interface accessibility

#### 12.3.2 Content Adaptation

* Support subtitles and audio descriptions
* Provide simplified interface versions
* Adapt to different ability needs

## 13. Contact Information

### 13.1 Customer Service Contact

For any questions or assistance needed, please contact us: - Customer service email: support@talenpal.com - Online customer service: Platform built-in customer service system - Business hours: Monday to Sunday 9:00-21:00

### 13.2 Legal Affairs Contact

For legal-related issues, please contact: - Legal affairs email: legal@talenpal.com - Privacy issues: privacy@talenpal.com - Intellectual property issues: ip@talenpal.com

### 13.3 Emergency Contact

Emergency situations (involving child safety): - Emergency email: emergency@talenpal.com

## 14. Effectiveness and Confirmation

### 14.1 Agreement Effectiveness

This Agreement takes effect from the date of publication and applies to all Platform users.

### 14.2 User Confirmation

Acceptance of this Agreement is indicated by any of the following methods: - Checking the “I have read and agree to this Agreement” option - Continued use of Platform services - Engaging in content creation activities

### 14.3 Parental Confirmation (for children under 13)

For child users, parents or guardians must: - Read this Agreement completely - Express agreement through verifiable means - Assume supervision and management responsibilities

**Important Reminder:**

This Agreement involves important rights and obligations for you and your children. Please carefully read all terms, especially those involving privacy protection, content creation rights, voice cloning technology use, and other aspects. If you have any questions, please contact our customer service team promptly.

We are committed to providing a safe, healthy, and beneficial content creation environment for users, especially child users. Thank you for your trust and support!

**Talenpal HK Limited**  
**September 20, 2025**