PRIVACY POLICY

Last Updated: 3rd June, 2025

1. Introduction

Normal Turtle Pty Ltd ("we," "us," or "our") operates the Super Scratch Party mobile application ("App"). This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our App.

We are committed to protecting your personal information and your right to privacy in accordance with applicable data protection laws, including:

- The General Data Protection Regulation (GDPR)
- The UK Data Protection Act 2018
- The Australian Privacy Principles
- The California Consumer Privacy Act (CCPA)

2. Information We Collect

2.1 Information You Provide

Username and Display Name Information: We collect your username or display name to identify you during game sessions and on leaderboards. This information is provided by you directly through user input and is stored temporarily in our Firebase Firestore database.

User-Generated Content: When you create custom quests, we collect and store the content you create, including text and game-related information. This content is used for gameplay purposes, feature development, and content moderation. All user-generated content is stored temporarily in our Firebase Firestore database.

In-App Purchase Information: We maintain records of your in-app transactions, including purchase preferences and payment verification tokens. This information is necessary for processing payments and maintaining transaction records as required by law.

2.2 Automatically Collected Information

Device Information: We generate and store a unique device identifier (UUID) on your device to assign a persistent local player identity. This identifier is stored in your device preferences and is not shared with external parties.

Technical Data: Our service automatically collects certain technical information necessary for operation, including your IP address (required for Firebase functionality), screen size and resolution (used for UI scaling), and error and crash reports for service improvement.

Usage Data: We collect information about how you interact with our App, including your game progress, statistics, and feature usage patterns. This information helps us understand how users engage with our App and allows us to improve the user experience.

3. How We Use Your Information

3.1 Core Functionality

Game Session Management: We use your information to manage active game sessions, maintain leaderboard functionality, and deliver custom quests to you and other players. This processing is essential for providing our core gaming services.

Transaction Processing: Your purchase information is used to facilitate in-app transactions, verify payments, and enable the restoration of purchases when necessary. This processing is essential for providing our paid services.

User Content Management: We process user-generated content to store and serve custom quests, perform content moderation, and develop new features based on user engagement patterns.

3.2 Service Improvement

Analytics and Performance: We analyze usage patterns, track errors, and monitor app stability to improve our services. This analysis helps us identify and resolve technical issues and enhance app performance.

User Experience Enhancement: We use collected data to optimize our interface, analyze feature usage, and improve overall app performance. This processing helps us provide a better gaming experience for all users.

4. Data Retention and Deletion

4.1 Retention Periods

Temporary Data: We maintain certain data for a 24-hour period, including usernames, display names, game session data, custom quest content, and game points and statistics. This temporary retention period helps maintain game functionality while protecting user privacy.

Extended Retention: We retain certain information for longer periods where necessary. Purchase records are maintained as required by applicable laws and regulations. Analytics data is retained for the duration of our service to support ongoing improvements. Error logs are kept for debugging purposes to ensure service stability.

4.2 Data Deletion

Automatic Deletion: Our system automatically deletes session data 24 hours after your game session ends. Custom quests are removed 24 hours after creation, and temporary cache data is cleared when you close the App. This automatic deletion helps protect your privacy and maintain data minimization.

User-Initiated Deletion: You may request deletion of your data by contacting us via email. Our team processes these requests manually and will provide confirmation once the deletion is complete. Please note that certain information may be retained if required by law or for legitimate business purposes.

5. Information Sharing and Disclosure

5.1 Third-Party Service Providers

Firebase Services: We use Firebase Core and Firestore for cloud hosting and data storage. These services process your username, game statistics, user-generated content, and IP address on global servers located in the United States and European Union.

Firebase Analytics processes usage patterns and interaction data to help us improve the App. This data is processed on servers in the USA and Europe.

Firebase Crashlytics monitors app stability by processing error reports and usage context data on global servers. This helps us identify and resolve technical issues promptly.

Payment Processing: For Apple users, we utilize Apple Pay and Apple Verify to process in-app purchases. These services handle purchase metadata and verification tokens on servers located in the US and EU.

For Android users, the Google Pay API processes similar purchase-related data on global servers. Both payment systems are subject to strict security measures and data protection standards.

5.2 Data Transfer Safeguards

International Transfers: When we transfer your data internationally, we implement appropriate safeguards including standard contractual clauses and data processing agreements. Where applicable, we comply with Privacy Shield requirements and other relevant data protection frameworks.

6. Data Security

6.1 Technical Measures

Transmission Security: We protect your data during transmission using industry-standard TLS/SSL encryption. All communications with our servers occur over secure HTTPS connections, and our API communications are encrypted to prevent unauthorized access.

Storage Security: All data stored in our systems is encrypted at rest using advanced encryption standards. We implement access controls and authentication measures to prevent unauthorized access to your information. Our security systems are regularly updated to address new security challenges.

Monitoring and Protection: We maintain continuous monitoring of our systems to detect and prevent security incidents. Our security measures are designed to protect against unauthorized access, alteration, disclosure, or destruction of your personal information.

6.2 Organizational Measures

Access Controls: We restrict access to personal information to authorized personnel only. Our team members are bound by confidentiality obligations and undergo regular privacy and security training.

Incident Response: We maintain incident response procedures to address any potential data security incidents promptly. In the event of a security breach affecting your personal information, we will notify you in accordance with applicable laws.

7. Your Rights

Depending on your location, you may have the right to:

- Access your personal information
- Correct inaccurate data
- Request deletion of your data
- Object to processing
- Data portability

To exercise these rights, contact us at: support@normalturtle.com

8. International Data Transfers

Your information may be transferred to and processed in countries other than your own. These countries include the United States, European Union member states, the United Kingdom, and Australia. We ensure appropriate safeguards are in place through:

- Standard contractual clauses approved by the European Commission
- Data processing agreements with service providers
- Compliance with regional data protection laws
- Implementation of appropriate technical and organizational measures

9. Children's Privacy

The App is not intended for users under the legal drinking age in their jurisdiction. We do not knowingly collect information from underage users. If we discover that we have collected personal information from an underage user, we will promptly delete such information.

If you believe we might have any information from or about an underage user, please contact us at support@normalturtle.com

10. Changes to This Privacy Policy

We may update this Privacy Policy periodically to reflect changes in our practices or for other operational, legal, or regulatory reasons. When we make material changes to this Privacy Policy, we will:

- Notify you through the App before the changes take effect
- Update the "Last Updated" date at the top of this Privacy Policy
- Obtain your consent where required by applicable law

11. Contact Us

For privacy-related questions, concerns, or requests:

- Email: support@normalturtle.com

12. Regional Privacy Rights

12.1 European Union and UK Residents

Under GDPR and UK data protection law, we act as the data controller of your personal information. The legal bases for processing your information are:

- Contract performance: Processing necessary for the performance of our agreement to provide you with the App's services
- Legitimate interests: Improving our services, maintaining security, and preventing fraud
- Legal obligations: Compliance with applicable laws and regulations
- Consent: Where specifically requested and provided by you

12.2 California Residents

Under the California Consumer Privacy Act (CCPA), California residents have specific rights regarding their personal information:

- Right to know what personal information is collected, used, shared, or sold
- Right to delete personal information held by businesses
- Right to opt-out of the sale of personal information (note that we do not sell personal information)
- Right to non-discrimination for exercising CCPA rights

12.3 Australian Residents

Under the Privacy Act 1988 and Australian Privacy Principles, you have rights regarding:

- Access to your personal information
- Correction of inaccurate information
- Making complaints about privacy breaches
- How your information is collected, used, and disclosed

You may lodge a complaint with the Office of the Australian Information Commissioner if you believe we have breached the Australian Privacy Principles.