Data Safety Policy for Community360 –Connect & Thrive

Introduction

At Community360 –Connect & Thrive, we prioritize the privacy and security of our users. This Data Safety Policy outlines the practices we follow to ensure that user data is handled with the utmost care and in compliance with relevant data protection laws and regulations.

Data Collection

1. Types of Data Collected

We collect the following types of data from users:

- **Personal Information:** Name, email address, phone number, etc.
- **Usage Data:** Information on how the app is accessed and used, including the pages visited, the time spent on each page, and other related statistics.
- **Device Information:** Device type, operating system, unique device identifiers, and mobile network information.
- **Location Data:** Approximate or precise location information, if permission is granted by the user.

2. Data Collection Methods

Data is collected through:

- User-provided information during account registration and profile setup.
- Automatic collection through the use of cookies, web beacons, and similar tracking technologies.
- User interactions with the app, such as form submissions, in-app purchases, and usage patterns.

Data Usage

We use the collected data for the following purposes:

- **Providing and Improving Services:** To operate, maintain, and enhance our app's functionality and user experience.

- **Personalization:** To tailor content and recommendations based on user preferences and interactions.
- **Communication:** To send notifications, updates, and promotional materials, with the user's consent.
- **Analytics:** To analyze usage trends and measure the effectiveness of our services and marketing efforts.
- **Compliance:** To comply with legal obligations and enforce our terms of service and other policies.

Data Sharing

We do not share user data with third parties except in the following circumstances:

- **With User Consent:** When users explicitly agree to share their data.
- **Service Providers:** With trusted third-party service providers who assist us in operating our app, conducting business, or serving our users, provided they agree to keep the data confidential and use it solely for the intended purposes.
- **Legal Requirements:** When disclosure is necessary to comply with a legal obligation, protect our rights, or prevent fraud or other illegal activities.

Data Security

We implement a variety of security measures to protect user data, including:

- **Encryption:** All sensitive data is encrypted during transmission and at rest.
- **Access Controls:** Access to user data is restricted to authorized personnel only.
- **Regular Audits:** We conduct regular security audits and vulnerability assessments.
- **Data Minimization:** We only collect and retain data that is necessary for the intended purpose.

To ensure transparency and comply with user data disclosure requirements, here is a detailed breakdown of the data collection and sharing practices relevant to apps:

1. Required User Data Types Collected and/or Shared

- **Personal Information**: Name, email address, phone number.
- **Location Data**: Precise or approximate location.
- **App Usage Data**: Interaction with the app, feature usage.
- **Contacts**: Access to contacts stored on the device.

- **Photos and Media**: Access to photos, media files, and other storage.

2. Data Sent Off the User's Device by Libraries or SDKs

- **Analytics SDKs**: Data such as user behavior, app performance metrics sent to analytics providers.
- **Advertising SDKs**: Data like user demographics and interests for targeted advertising.
- **Crash Reporting SDKs**: Data on app crashes and errors sent to crash reporting services.
- **Social Media SDKs**: User information shared with social media platforms for integration purposes.
- **Payment SDKs**: Transaction details sent to payment processing services.

3. Data Transferred to Third-Party Apps on the Same Device

- **Single Sign-On (SSO) Services**: Data used for authentication across multiple apps.
- **Payment Services**: Data shared with other payment apps for transaction processing.

4. Data Collected or Transferred Through Webview

- **Embedded Web Content**: Data collected via embedded web pages, including cookies and user interactions.
- **Third-Party Content**: Data transferred when interacting with third-party content within the app's webview.

Important Considerations

- **User Consent**: Always obtain user consent before collecting or sharing any data.
- **Data Security**: Ensure robust security measures are in place to protect user data.
- **Transparency**: Clearly communicate data practices in the app's privacy policy and user agreements.
- **Regulatory Compliance**: Adhere to regulations like GDPR, CCPA, and others relevant to your user base.

User Rights

Users have the following rights regarding their data:

- **Access:** Users can request access to the personal data we hold about them.
- **Correction:** Users can request corrections to inaccurate or incomplete data.
- **Deletion:** Users can request the deletion of their data, subject to legal and contractual restrictions.
- **Objection:** Users can object to the processing of their data in certain circumstances.
- **Portability:** Users can request a copy of their data in a structured, commonly used, and machine-readable format.

Changes to This Policy

We may update this Data Safety Policy from time to time. Users will be notified of any significant changes through the app or via email.

Contact Us

If you have any questions or concerns about this Data Safety Policy, please contact us at info@community360.au