

Privacy Policy of Kidsafety

Last Updated: 2026/07/01

1. Introduction

This Privacy Policy (“Policy”) explains how SIN FREEMAN, a sole proprietor registered in Hong Kong and the operator of Kidsafety (<https://kidsafety.net/> and the Kidsafety mobile service), collects, uses, stores, shares, and protects information.

This Policy applies to the services provided and controlled by SIN FREEMAN, including:

- the Kidsafety mobile application, including its parent-facing functions and the companion component used on a child’s device (the “App”), distributed through Google Play;
- the website available at <https://kidsafety.net/> and any related subdomains or official promotional pages (the “Website”);

(together, the “Services”).

By using the Website, creating an account, pairing devices, or using the Services, you confirm that you have reviewed this Policy. If you do not accept it, do not use the Services.

Kidsafety is a parental control and family digital-wellbeing service. It helps parents and legal guardians review device use, set screen-time limits and schedules, and keep important communication or educational functions available. It is not designed for secret or unlawful surveillance.

We aim to collect only necessary information and use appropriate safeguards. This Policy reflects the Hong Kong Personal Data (Privacy) Ordinance and other applicable requirements, including the GDPR where relevant.

Questions about this Policy or the handling of personal information may be directed to the contact details in Section 17 (Contact Information).

2. Information We Collect

Kidsafety collects information needed for pairing, parental controls, subscriptions, support, security, and improvement. We do not intentionally collect unrelated information.

2.1 Information Provided Directly by You

When you register, configure Kidsafety, or contact us, you may provide:

- **Account Information:** an email address, account name, password or authentication details, and optional profile information used to identify the parent or guardian account.

- **Payment Information:** subscription status, product identifiers, purchase tokens, and confirmations from Google Play Billing. We do not store full bank-card details.
- **Family Setup Information:** device names, optional child profile labels, pairing codes, schedules, limits, and the applications selected for management.
- **Communications:** support requests, feedback, attachments, and other messages submitted through the App, Website, or by email to support@kidsafety.net.

2.2 Information Collected Automatically

Certain technical and service information may be generated when the Services are used:

- **Device Information:** device model, operating system, language, App version, installation identifier, and identifiers needed to pair managed devices.
- **Usage and Control Data:** screen time, application names and usage duration, timestamps, limits, schedules, pairing status, feature use, and restriction status.
- **Log and Diagnostic Data:** IP address, access time, crash reports, errors, security events, and performance information.
- **Cookies and Similar Technologies (Website only):** used for essential operation, preferences, analytics, and advertising measurement where permitted.

2.3 Information from Third Parties

We may obtain limited information from service providers that support Kidsafety:

- **Google Play Services:** installation information, subscription status, purchase verification, refunds, and other billing confirmations;
- **Analytics and Diagnostic Providers:** aggregated, pseudonymous, or technical data relating to usage, stability, errors, and performance;
- **Advertising Platforms (including Google Ads):** campaign, referral, and conversion information that is not intended to directly identify an individual user.

We do not buy lists of personal information. Information received from third parties is used only for the purposes described in this Policy.

3. How We Use Your Information

We use information to provide, secure, maintain, and improve Kidsafety, including for the following purposes:

3.1 Service Operation and Functionality

- To create accounts, authenticate users, pair authorised family devices, and maintain their connection;

- To calculate screen time and application-use statistics and apply limits, schedules, and permitted-app settings;
- To validate subscriptions and in-app purchases made through Google Play and provide the corresponding premium functionality;
- To synchronise settings and service status across paired devices and provide operational notices;
- To answer questions, troubleshoot setup, and provide customer support.

3.2 Personalization and Improvement

- To remember family settings, schedules, and selected applications;
- To improve setup, interface design, compatibility, and family-safety features;
- To identify errors, improve compatibility with Android devices, and enhance stability and performance.

3.3 Security and Fraud Prevention

- To identify suspicious access, fraud, misuse, or interference with pairing and parental-control settings;
- To protect the integrity of the Services, paired devices, user information, and subscription entitlements;
- To enforce our Terms of Service and prevent prohibited, unlawful, or abusive use.

3.4 Legal and Compliance Purposes

- To meet obligations imposed by applicable Hong Kong and international laws;
- To respond to valid legal processes and lawful requests from competent authorities;
- To establish, exercise, or defend our legal rights and protect users, the business, and the Services.

Kidsafety does not sell or rent personal information. We process information for disclosed purposes in a lawful, fair, and proportionate manner.

4. Legal Basis for Processing Personal Data

Where the GDPR or similar laws apply, Kidsafety processes personal information only when an appropriate legal basis exists.

Depending on the circumstances, we rely on the following legal bases:

4.1 Performance of a Contract

Processing is necessary to provide the Services requested by the account holder, including:

- registering and maintaining a parent or guardian account;
- pairing devices and delivering screen-time, scheduling, reporting, and restriction functions;
- verifying subscriptions, restoring purchases, and enabling paid features;
- providing technical assistance and responding to service requests.

Without essential information, some Kidsafety functions may be unavailable.

4.2 Consent

We rely on consent where consent is required, including for:

- sending optional marketing or product communications;
- using non-essential analytics, advertising identifiers, or similar technologies where local law requires permission;
- accessing Android permissions or device capabilities that the user must actively enable during setup;
- placing non-essential cookies or comparable technologies on the Website.

Consent may be withdrawn through settings or by contacting us, without affecting earlier lawful processing.

4.3 Legitimate Interests

We may process limited information for legitimate interests that do not override user or child rights, including:

- maintaining, improving, and measuring the reliability and usability of Kidsafety;
- protecting accounts, preventing fraud, and securing paired-device communications;
- developing features that support transparent and responsible family device management.

4.4 Legal Obligations

Information may be processed or retained where necessary to comply with legal and regulatory duties, including:

- tax, accounting, record-keeping, and consumer-protection requirements;
- responding to binding requests, court orders, or other lawful demands from authorities.

4.5 Vital Interests

In exceptional cases, limited information may be processed to address an immediate security risk or protect vital interests.

We limit processing to what is reasonably necessary and explain material practices to users.

5. Data Sharing and Disclosure

We do not sell, rent, or trade personal information. Limited disclosure may occur as described below.

5.1 Service Providers and Technical Partners

We may use selected providers to support Kidsafety, including:

- Cloud hosting and infrastructure services used for secure processing, synchronisation, and storage;
- Google Play Billing and related Google services used to distribute the App, verify purchases, and manage subscriptions;
- Analytics, crash-reporting, and performance tools used to identify errors and improve reliability;
- Customer-support and communication tools used to receive and respond to user requests.

Providers processing information for us are expected to:

- use information only for the agreed and documented purpose;
- apply confidentiality and access-control requirements;
- maintain reasonable technical and organisational safeguards;
- comply with applicable privacy and data-protection obligations.

5.2 Business Transfers

If Kidsafety or its assets are reorganised, acquired, financed, or transferred, relevant information may form part of the transaction. Users will be notified where required.

5.3 Legal Requirements and Protection

We may disclose information where we reasonably believe disclosure is necessary to:

- comply with applicable law, legal process, or a binding regulatory obligation;
- respond to a valid request from a court, regulator, or law-enforcement authority;
- protect the rights, property, safety, and security of users, children, SIN FREEMAN, or the Services;
- investigate fraud, abuse, security incidents, or violations of our Terms of Service.

5.4 Aggregated and Anonymized Data

We may use or share aggregated or anonymized statistics that do not reasonably identify a user or child for analytics, planning, research, or improvement.

We select providers with appropriate safeguards and disclose material sharing categories in this Policy.

6. Data Retention

Kidsafety retains information only as long as needed for service delivery, security, legal duties, disputes, and agreement enforcement. Periods vary by data type and purpose.

6.1 General Retention Principles

- **Account Information:** kept while the account is active, then deleted or de-identified after a valid deletion request unless retention is legally required.
- **Payment and Transaction Data:** confirmations and accounting records may be retained for billing, fraud, tax, and compliance. Kidsafety does not store full card details.
- **Family and Device Data:** pairing records, settings, schedules, usage statistics, and managed-app data are kept while needed for family-control functions, then deleted or anonymized subject to backups and legal duties.
- **Support Communications:** normally retained for up to 12 months, or longer for unresolved issues, security matters, or legal requirements.

6.2 Marketing and Communication Data

Optional communication data is retained until consent is withdrawn, the user unsubscribes, or it is no longer needed. Limited suppression records may preserve opt-outs.

6.3 Technical and Log Data

Logs, crash reports, diagnostics, and security records are generally retained for 6–12 months unless needed for an investigation or legal requirement.

6.4 Legal and Regulatory Requirements

Some records may be retained longer where required for tax, accounting, disputes, consumer protection, or regulation.

6.5 Secure Deletion and Anonymization

When information is no longer needed, we delete, overwrite, or de-identify it. Protected backup copies may remain until routine deletion cycles finish.

We retain information only for a justified operational, security, or legal purpose.

7. International Data Transfers

Information may be processed in Hong Kong or other countries where our infrastructure and providers operate.

7.1 Locations of Processing

Depending on the services used, information may be processed in:

- Hong Kong and the European Economic Area (EEA);
- the United States;
- other jurisdictions in which an authorised cloud, analytics, support, or platform provider maintains facilities.

Those locations may apply different privacy laws from the user's country of residence.

7.2 Safeguards for Transfers

Where required, cross-border safeguards may include:

- approved contractual clauses, including Standard Contractual Clauses where relevant;
- data-processing terms and confidentiality obligations with providers;
- encryption, restricted access, authentication controls, and secure technical infrastructure.

7.3 User Acknowledgment

Using Kidsafety may require information to be processed outside the user's country where necessary to provide the Services.

We apply this Policy regardless of location and seek providers with appropriate privacy and security practices.

7.4 Third-Party Providers

Providers that process information for Kidsafety are expected to:

- act only for defined service purposes and in accordance with applicable instructions;
- use reasonable security, confidentiality, and access-control measures;

- comply with the privacy laws and contractual protections relevant to their processing.

We assess transfers with the aim of maintaining practical protection for user information.

8. Data Security

Kidsafety uses technical, organisational, and administrative safeguards against loss, unauthorised access, alteration, disclosure, and misuse. Measures are reviewed as risks evolve.

8.1 Technical Safeguards

- **Encryption:** communications between supported devices, the App, and our servers are protected in transit using secure protocols such as TLS.
- **Secure Infrastructure:** systems are hosted in controlled environments that may include firewalls, monitoring, separation of services, and provider security controls.
- **Access Controls:** access to personal and family information is restricted according to role, operational need, and authentication requirements.
- **Monitoring and Testing:** logs, security reviews, software updates, and vulnerability remediation are used to identify and address threats.
- **Data Integrity and Backup:** reasonable backup and recovery procedures are maintained to reduce the risk of accidental loss and support service continuity.

8.2 Organizational Measures

- **Confidentiality Obligations:** personnel and contractors who may handle user information are subject to confidentiality expectations and limited-access rules.
- **Internal Procedures:** operational rules cover access, support handling, retention, deletion, incident escalation, and responsible use of information.
- **Incident Response:** suspected incidents are assessed, contained, investigated, and corrected. Notifications are made where required by law.

8.3 User Responsibility

Users also contribute to account and device security. Account holders should:

- keep passwords, pairing codes, and account credentials confidential;
- use strong, unique passwords and protect access to the parent device;
- review paired devices and remove access that is no longer authorised;
- contact us promptly if account compromise or unauthorised pairing is suspected.

No electronic transmission, mobile device, or storage system can be guaranteed completely secure.

9. Your Rights

Depending on applicable law, users may have privacy rights under the GDPR, the Hong Kong Personal Data (Privacy) Ordinance, or similar laws.

9.1 Right of Access

You may ask whether we process your information and request access to eligible information and an explanation of its use.

9.2 Right to Rectification

You may request correction or completion of information that is inaccurate, incomplete, or out of date.

9.3 Right to Erasure

Where the law provides, you may request deletion of personal information when:

- the information is no longer required for the purpose for which it was collected;
- consent is withdrawn and no other lawful basis supports the processing;
- the processing is unlawful or deletion is otherwise required by law.

9.4 Right to Restrict Processing

You may request restricted processing in certain cases, including while accuracy or lawfulness is reviewed.

9.5 Right to Data Portability

Where required and feasible, you may request eligible information in a common machine-readable format or ask for transfer to another provider.

9.6 Right to Object

You may object to legitimate-interest processing or direct marketing. We will stop processing where required.

9.7 Right to Withdraw Consent

Where processing relies on consent, you may withdraw that consent at any time through available settings or by contacting us.

9.8 Automated Decision-Making

Kidsafety does not make legally or similarly significant decisions solely through automated processing. If this changes, appropriate information and rights will be provided.

We aim to honour valid requests, subject to identity checks, legal limits, and the rights and safety of other family members.

10. Exercising Your Rights

Kidsafety provides a direct process for eligible privacy requests.

10.1 How to Submit a Request

Requests relating to the rights described in Section 9 may be sent to:

- Email: support@kidsafety.net

Please include a clear description of the request and use a subject such as “Privacy Request” so that it can be routed appropriately.

To protect users and children, we may verify the requester’s identity and authority. Verification data is used only for the request and retained only as necessary.

10.2 Response Timeframes

We aim to acknowledge and respond to valid requests within 30 calendar days, or within another period required by applicable law.

Complex requests, multiple family devices, or additional verification may justify an extension where allowed by law. We will explain material delays.

10.3 Limitations

A request may be limited or refused where:

- fulfilment would adversely affect the privacy, safety, or legal rights of another person, including a child or another account holder;
- retention or processing is required by law, necessary for security, or needed to establish or defend legal claims;
- the request is manifestly unfounded, excessive, repetitive, or cannot be reliably verified.

Where permitted, we will explain any refusal or limitation.

10.4 Fees

Standard requests are free. A reasonable fee may apply to clearly excessive or repetitive requests where law permits.

10.5 Complaints

You may contact us about suspected improper handling and may also complain to the competent privacy authority.

We encourage users to contact us first so we can investigate promptly.

11. Cookies and Similar Technologies

The Website may use cookies, pixels, local storage, and similar technologies for operation, preferences, analytics, and advertising measurement.

11.1 What Are Cookies

Cookies are small files placed on a browser or device to support sessions, preferences, security, analytics, and measurement.

11.2 Types of Cookies We Use

- **Strictly Necessary Cookies:** support essential security, navigation, consent, and Website functionality;
- **Performance and Analytics Cookies:** help us understand page visits, errors, and how visitors use the Website;
- **Functional Cookies:** remember choices such as language, display settings, or previously selected preferences;
- **Advertising and Measurement Cookies:** may record campaign referrals and conversions and help evaluate advertising effectiveness;
- **Third-Party Cookies:** may be set by approved analytics, hosting, security, or advertising services integrated with the Website.

11.3 Cookie Management

Cookies may be blocked or removed in browser settings, but some Website functions may then be unavailable.

11.4 Consent

Where required, non-essential technologies are used only after consent, which may later be withdrawn.

11.5 Cookies in the App

The App does not rely on browser cookies for core functions. It may use secure local storage, preferences, tokens, and system identifiers for login, pairing, settings, and reliability.

12. Tracking, Analytics, and Third-Party Tools

Kidsafety uses limited analytics, diagnostic, advertising, and platform tools to measure performance, reliability, discovery, and use.

12.1 Purpose of Analytics

Analytics and diagnostic tools may be used to:

- understand navigation and feature use in the parent-facing App and Website;
- measure screen flows, setup completion, subscription events, and general performance;
- detect crashes, connection failures, permission problems, and technical errors;
- improve instructions, compatibility, stability, and overall usability;
- measure campaign referrals and the effectiveness of advertising.

Where possible, analytics is aggregated or pseudonymized and is not used to read calls, messages, or private communications.

12.2 Types of Tools Used

Kidsafety may use services such as:

- Google Analytics or Firebase services for aggregated usage measurement, diagnostics, notifications, and crash reporting;
- Google Ads conversion measurement to understand whether advertising leads to Website visits, Google Play visits, installations, or other defined actions;
- Performance and security-monitoring tools used to identify service interruptions, abuse, and compatibility issues.

Tools are configured to limit collection to information relevant to their stated purpose.

12.3 Data Collected by Analytics Tools

Depending on configuration and user choices, analytics data may include:

- device category, operating-system version, App version, and language;
- approximate region derived from an IP address, rather than precise GPS location;
- session duration, screen views, feature interactions, errors, and subscription events;
- pseudonymous installation, analytics, or advertising identifiers where permitted.

We do not intentionally provide analytics providers with names, support-message content, or private child communications.

12.4 Advertising and User Control

The free version may show advertising. Ads in parent-facing areas may be provided by third-party networks under applicable platform and privacy rules.

Users can manage advertising and privacy preferences through Android, Google, browser, and App settings.

- Tracking may also be limited by rejecting non-essential cookies, resetting permitted identifiers, or using platform-provided privacy controls.

12.5 Transparency and Responsibility

We disclose the main analytics and tracking categories and expect providers to process information only for defined purposes under appropriate safeguards.

Our aim is to improve and support the Services without selling personal information or using analytics for covert monitoring.

Analytics and advertising help maintain the Services and fund limited free access; they are not used to sell personal information or conduct covert monitoring.

13. Third-Party APIs & Integrations

Kidsafety uses selected services for App distribution, infrastructure, synchronisation, notifications, billing, and diagnostics while limiting transferred information.

13.1 Purpose of Integrations

Integrations are used where reasonably necessary for core functions and reliable operation.

13.2 Services Enabled by Integrations

Third-party APIs and platform functions may support:

- secure account authentication, device pairing, and synchronisation of selected family settings;
- cloud hosting, notifications, error reporting, and temporary processing needed to deliver the Services;
- subscription purchase, restoration, and validation through Google Play Billing;
- optional actions initiated by an adult account holder, such as opening Google Play or contacting support.

13.3 Data Handling Principles

When Kidsafety exchanges information with an authorised integration:

- only information reasonably required for the function is transferred;
- communications are protected through encrypted connections where technically supported;
- information must not be used by the provider for unrelated purposes except as independently disclosed and legally permitted;
- providers are expected to maintain confidentiality, access controls, and appropriate security measures.

13.4 Types of Third-Party Services

Kidsafety may rely on categories of services including:

- Google services, such as Google Play, Firebase, billing, notifications, diagnostics, and related Android platform functions;
- cloud hosting and database infrastructure used for secure processing, synchronisation, and service availability;
- analytics, crash-reporting, customer-support, and security tools used to maintain and improve operation.

Providers are selected with regard to their function, reliability, security practices, and applicable contractual or legal requirements.

13.5 User Control

Users can manage integrations through permissions, Android settings, account controls, and subscription settings. Revoking access may disable a related function.

Integrations support Kidsafety functions and do not authorise hidden surveillance, unrelated profiling, or unrestricted access to family information.

14. App Store & Google Play Compliance

Kidsafety is maintained with the intention of following applicable Google Play policies, user-data rules, payment requirements, and Android permission standards.

14.1 Policy Compliance

Our compliance approach includes consideration of:

- Google Play User Data, privacy, disclosure, and Data safety requirements;
- Google Play payment requirements for subscriptions and in-app digital features;
- app-content, advertising, permission, and family-related requirements that apply to the Services.

We review product descriptions, disclosures, permissions, integrations, and Website information as the Services and platform rules change.

14.2 Content Standards

Kidsafety is not intended to promote or enable:

- misleading claims, impersonation, or deceptive representations of the product;
- unlawful, covert, or unauthorised surveillance of adults or children;
- content or activity that violates intellectual-property rights or applicable law.

Kidsafety is designed for transparent family rules concerning screen time and application use.

14.3 Permissions and Data Transparency

The App may request Android permissions necessary for parental-control functions, such as:

- usage-access or equivalent permission to calculate screen time and application-use statistics;
- accessibility, display-over-other-apps, background operation, autostart, or device-administration capabilities used to apply limits, show notices, maintain schedules, and protect authorised settings;

Permissions must be enabled through Android controls and may be revoked, although related functions may stop working.

14.4 Accurate Representation

Our Website, ads, screenshots, and Google Play materials are intended to describe actual Kidsafety functions without unrealistic promises.

14.5 Security and Integrity

We design and maintain the Services so that:

- the App does not contain intentionally malicious code or hidden functionality;
- Kidsafety does not provide a covert mode for secretly reading messages, recording calls, activating a microphone or camera, or monitoring an adult without authorisation;
- third-party components are reviewed and configured for their stated operational purposes.

We monitor platform requirements and seek to address security, privacy, and compliance issues promptly.

15. Children's and Family Privacy

Kidsafety is offered to parents and legal guardians. A companion component may operate on a child's device under the adult account holder's direction.

15.1 Adult Account Holders and Guardian Responsibility

Children should not create a parent account, purchase subscriptions, or configure monitoring. The adult must have authority to connect the device and provide any required notice or consent.

15.2 Limited Child-Device Information

Kidsafety may process device identifiers, installed-app names, usage duration, screen time, schedules, restriction status, and diagnostics from a connected child device. It is not intended to collect private call or message content.

15.3 Protective Measures

If we learn that a child's information has been processed without appropriate adult authority or in a manner inconsistent with this Policy, we may:

- delete or de-identify the affected information where reasonably possible;
- disconnect the device, restrict the account, or request additional verification from the adult account holder.

Parents or guardians may contact support@kidsafety.net about deletion, unauthorised use, or child-device privacy.

16. Amendments to This Privacy Policy

We may update this Policy for changes in functionality, law, platform rules, providers, or business practices.

16.1 Notification of Changes

Material changes may be communicated through:

- a notice or updated Policy published on the Website;
- an in-app notice or message presented to the adult account holder;
- an email notification where appropriate and where contact permission is available.

The date at the top identifies the current version.

16.2 Nature of Changes

Revisions may include:

- clarifications intended to make existing practices easier to understand;
- changes needed to address new laws, regulatory guidance, or platform requirements;
- updates relating to new features, permissions, providers, or technical integrations;
- changes to business, support, ownership, or contact information.

We will not materially expand use of previously collected information through an update without any notice or consent required by law.

16.3 Continued Use

Continued use after an update indicates an opportunity to review it, subject to any additional consent required by law.

If you reject a material change, you may stop using Kidsafety, disconnect devices, cancel through Google Play, and request deletion of eligible information.

17. Contact Information

Questions, privacy requests, or concerns regarding this Policy or the handling of personal information may be submitted using the contact information below:

Legal Entity: SIN FREEMAN (Sole Proprietor, Hong Kong)

Registered Address:

Flat 7, 3/F
28 Baker Street
Hung Hom
Hong Kong

Email: support@kidsafety.net

Phone: +852 9779 0124

We aim to respond to legitimate privacy requests within a reasonable period, ordinarily 30 calendar days, subject to verification and applicable law.

You may also contact the Privacy Commissioner for Personal Data in Hong Kong or another competent authority.