FAMILY ZONE

PRIVACY POLICY

Contents

21 INTRODUCTION

1.1 Our commitment

We are committed to protecting the privacy of our customers. This Privacy Policy describes how we collect, store, use and distribute information. We also set out your options which include how you can avoid capture of certain information and how you can access and update certain information.

If you do not agree with this policy, please do not access or use our Products or interact with any other aspect of our business.

When you sign up with us you will be presented an opportunity to review this policy. If you continue then we are entitled to assume you have consented to this policy.

1.2 Meaning of terms

Unless otherwise specified in this policy, terms have the same meaning as set out in our Customer Terms. In particular:

(a) **Account** means an account with us. An account is where in our Products you can manage your settings, subscription, purchases and support. An account holder is the party responsible (under agreement with us) for the account, irrespective of whom is paying.

(b) **End User** refers to users affected by our Products (eg through device management or filtering).

(c) **Operational Service Providers:** Means third parties whom work for us to help us provide our Products to you, They provide services including website and application development, hosting, maintenance, backup, storage, virtual infrastructure, payment processing, analysis, customer, technical and sales support.

(d) **Operational Purposes:** Refers to matters which are fundamental to the operation of our Products. Information is collected, processed or shared for Operational Purposes where it allows us to: make the Products and features you have requested from us available to you; bill you; deliver Products to you; get in contact with you when we reasonably need to; enforce our agreement with you; respond to enquiries and requests from you; support our efforts to monitor and improve the features, performance and quality of our Products; and comply with relevant laws.

(e) **Parents** refers to the parents or guardians of an End User.

(f) **Products** means the cyber safety and security products and services that we provide customers, either directly or through resellers,

and includes without limitation our Websites, Services, Hardware, Software, Consulting, API's, Support and Documentation.

(g) **Resellers** means third parties whom sell our Products to customers on our behalf.

(h) **Legitimate Business Reasons** means in relation to an act of a party, that party's compliance with contractual obligations and applicable laws and regulations, and in particular those relating to privacy.

(i) **School** means the provider of educational services including the organisations, associations and government agencies responsible.

(j) **Services** means our cyber safety and security services.

(k) **Service Partners** means third parties whom we introduce to you but deliver services directly to you such as Cyber Experts and third party providers technology and equipment.

(l) **You** and Your refers only to the account holder of the Products we provide.

(m) **we**, **our** or **us** means any Family Zone corporate entity (including Family Zone Cyber Safety Limited ABN 33 167 509 177 (Australia), and Family Zone Inc (USA), our assignees, successors and any subcontractor engaged by, us to provide the Products.

1.3 General privacy principles

In the course of our business we may collect information from and about you, your End Users and the use of our Products. In general:

- Data that relates to or identifies you or your End Users is owned by you;
- User Content such as content submitted by you into forms or surveys is owned by you; and
- Data associated with your use of our Products is owned by us.

Where we collect information owned by you (in accordance with this policy) you permit us to use it in accordance with this policy.

We collect and process information about you only where we have legal basis for doing so. We collect, use and process your information only where:

- We need it to provide, operate, support, personalize and protect the Products you have requested from us;
- We have a Legitimate Business Reasons for doing;
- You have given us consent to do so for any other specific purpose; or
- We need to do so to comply with a legal obligation.

You have the right to know what we collect and have collected about you. You have the right to know what we do with your information and you have the right to opt-out of providing us information and the right to request its removal. We may however not be able to provide you with our Products in these circumstances.

1.4 Interpretation of this policy for 'paid accounts'

On occasion, accounts with us may be purchased by a separate party. For example, an enterprise or a school may purchase a subscription to our Services on behalf of an employee's or a student's family.

In such circumstances then you (or your) in this policy means the account holder, irrespective of who pays for the subscription.

Please note that an account holder's relationship with third parties (such as schools, resellers or other enterprises) can affect the information we share about them as set out in this policy.

22 THE INFORMATION WE COLLECT

2.1 Account Information

When you sign up with us we will ask for contact information to enable us to establish an account. This will include name, contact details, username and security information such as a password and PIN.

We will hold this information for as long as reasonably necessary.

This information is required to provide you with Services. You can access and modify this information directly through your account.

2.2 Address Information

We do not typically seek your address details however we may ask for them if:

(a) you order a physical Product;

(b) You request on-site support to be delivered to your premises;

(c) Our payment provider requires your address, post code or zip for verification purposes.

We will not use this information for any other purpose.

We will hold this information for as long as reasonably necessary or until you ask for us to remove it.

You may choose to have deliveries sent to another address eg a post office. You can ask us to delete your address information at any time.

2.3 Information you provide to support

When you use our support channels you may share with us information in emails and support tickets or over the telephone or in online chat services. We will capture this information as a record of what we've been asked to and have done for you. We do this for quality assurance purposes.

We will hold this information for as long as reasonably necessary or until you ask for us to remove it.

This information is required to provide you with our Products. You can ask us to delete it.

2.4 Payment Method

If you are paying us via electronic funds transfer, we will need to ensure you set up a payment method (such as a credit card). We do not store this information. We will pass you to a compliant payment gateway.

You can access, change and remove your Payment Method through your account, where we'll direct you to our third party gateway.

2.5 Your Time Zone

When you sign up we require capture of your time zone. If we can, we will estimate this through geo-IP (through your internet session). We need time zone to enable us to pre-configure our Products for you and for your account to function.

You can access and change this in your account.

2.6 Registering Your End Users

End Users are those persons that are affected by our Services (eg authentication, filtering, device management). End Users may be students (at a school), your children, guests on your network, your staff or you.

When you register End Users we will ask for their name and date of birth. Date of birth helps us pre-configure settings for them. We ask for additional optional information if you want to use optional features such as a security PIN (for device borrowing) and the name of the school they attend (for school community collaboration).

When devices such as tablets and personal computers connect to our Services we will ask you to register them. We'll ask for the device type, a device name and for its End-User to be identified. This is optional.

We will hold this information for as long as reasonably necessary.

This information is required to provide you with Services. You can access, modify and delete this information directly through your account.

2.7 End User Avatars

In some of our Products you may be permitted to add pictures for your End Users. This is optional.

We will hold this information for as long as reasonably necessary or until you ask for us to remove it.

This information is optional. You have the choice to load photos of your End Users, avatars; other graphics or not use this feature. You have access to modify and remove this information directly through our Products.

2.8 End User Cyber Safety Data

Our Products enable you to monitor and control End User's use of the internet and devices. This includes their use of networks and devices not owned by you.

Our Products necessarily capture usage and device information ("Cyber Safety Data") so we can provide this control and insight to you.

We will hold this information as long as reasonably necessary. This is typically 30 days after which time we will de-identify it. You can access this information directly through your account.

The following table outlines what we collect and your options.

Data Type	Description	Your options
Internet Usage	Use of the internet including online search terms, sites visited and blocked and related meta-data such as device, protocol, website, location, time and date.	You can disable tracking of this information for specific End Users (other than guests on your network) in your account (in User Settings). Doing so means we can still apply internet filters however we will not store the usage records. By default, users aged 18 and over are set to be not-tracked by us.
Mobile Apps	Use of applications, including what applications are installed or attempted to be installed, are used and for how long, are blocked or permitted to be used and related information such as device details, time and date.	This data is fundamental to the operation of our Mobile Zone Services. You can choose to not install Mobile Zone however device management and on-device filtering will not be available to you.
Device Location	Geo-location information derived from GPS services available on smart devices.	You can disable location services on the mobile devices that have our Mobile Zone App installed. Doing so will affect the performance of our filtering service.

Behaviour	Our Products allow identification of actions (or patterns of actions) which are indicative of misbehaviour or notable behaviour. For example, if an End User deletes our Mobile Zone App without approval. Such actions can be logged by us and made available to you.	You can disable tracking of this information for specific End Users in your account (in User Settings). This means we will not log these actions or store this data.
Transactional	Our Products log certain transactions for the purpose of notifying and reporting system events. For example, where a device connects to your network or an End User seeks to borrow a device.	Transactional data is required for the function of our Products. You can disable some events from being monitored in your account (in Controls).

2.9 Submissions (Feedback, suggestions, survey responses and forums)

We may provide opportunities to post submissions in a forum, comments in a blog or a wiki, or to complete surveys and forms (resources). If these resources are identified as public or having a membership group then the membership of the relevant resource will have access to your submissions. If the resource is public then your submissions will be public. We are not responsible for third party use of information submitted by you in these circumstances.

This information is offered voluntarily. You may ask us to de-identify it.

2.10 Credit Information (Corporate and organizations)

If you are a company or an unincorporated organization we will ask you to provide us with information about your organization such as your business and tax registration details and trading address. We do this only for the purpose of compliance with applicable trade and taxation laws and for verification purposes.

We may also source information publicly available or properly available for these purposes from credit reporting, law enforcement or government agencies.

We will hold this information in accordance with standard business records practice, which is typically 7 years.

2.11 Diagnostic Information

Our Products log system level activities. We capture this information for quality assurance purposes only. It is stored for less than 30 days and typically a lot less.

We are unable to provide system logs to you.

2.12 Web Analytics

Like most organizations, we use automatic data collection technology (such as Google Analytics) when you visit our websites. We may collect information such as your IP address, Internet service provider, browser type, operating system and language, referring and exit pages and URLs, date and time, amount of time spent on particular pages, what sections of the website you visit, number of links you click while on the website, search terms, and other data.

This information is collected automatically and anonymized. By accessing and using our website, you consent to the processing of this data by our analytics partners in the manner and for the purposes set out in this policy.

Analytics are collected through services we obtain from 3rd party providers, such as Google. Where possible we will provide at familyzone.com/tracking details of our providers and guidance on how to opt-out from data collection.

2.13 Cookies and other Tracking Technologies

We and our advertising and analytics partners, use cookies and other tracking technologies (e.g., web beacons, device identifiers and pixels) to provide functionality and to recognize you across different services and devices.

We will not use them to market third party products or to gather information on you or your End Users to sell to others.

For more information, please see our Cookies and Tracking Notice below or visit familyzone.com/tracking.

2.14 Third party authentication services

For your convenience we may offer you the ability to sign in to our Products using third party authentication services provided by organizations such as Google and Facebook. Where you choose such services, we will exchange authentication information with them such as your email address. You will be required to accept their terms of use and policies with respect to the exchange of information.

We only use these services for the purpose of authentication.

You may disable authentication services at any time through your account.

2.15 Sensitive Information

Certain legal jurisdictions define Sensitive Information and prescribe rules around it's capture, storage and use. For the purpose of this Privacy Policy we define Sensitive Information to mean information or an opinion about an individual's:

- Racial or ethnic origin;
- Political opinion;
- Membership of a political association;
- Religious beliefs or affiliations;
- Philosophical beliefs;
- Membership of a professional or trade association;
- Membership of a trade union;
- Sexual preferences or practices; or
- Criminal record.

Unless permitted by law and requested by you or required by law, we will not record or use Sensitive Information.

2.16 Resellers

We provide our Products through resellers such as telecommunications companies and technology vendors. If you have purchased our Products through a reseller then they may pass to us your account set up information and in some circumstances End User and device registration information. We require our resellers to have authorisation from you before doing so.

We will hold this information passed to us by resellers as long as reasonably necessary.

If you didn't consent to the creation of your account you can cancel it in your account, through your provider or by contacting us.

2.17 Information from other users

In some limited circumstances other users of our Products may provide information about you. For example, a school may pre-register an account for you or another customer may refer your email to us because they believe you may be interested in our Products.

We require these parties to confirm to us that they have your permission to do this.

If you didn't consent to this action, please contact us per the contact details set out below.

23 HOW WE USE YOUR INFORMATION

3.1 How we use your information

How we use the information we collect depends on the information and Products you use. Below are the specific purposes for which we use the information we collect.

- To provide you with the features available in our Products;
- To deliver you physical Products;
- To direct third parties to you where you have requested us to do so;
- To personalize your experience;
- To bill and take payments from you;
- To let you know about events which we reasonably believe you need to know about or you have asked us to tell you about;
- To provide you with advice and details on features and offers we reasonably believe may be of interest to you;
- To let you know about third party services (subject to your opt-in) we believe you may be interested in;
- To monitor and analyse the quality and performance of our Products and customer satisfaction with them;
- To support our ongoing research and development efforts;
- To support our Products including resolving queries and technical issues, troubleshooting and repairing our Products;
- To support our security measures (such as verifying accounts and activity); and
- To comply with relevant laws and regulations and to protect our legitimate legal rights.

With your consent we may use information about you for specific purpose not listed above. For example, we may publish testimonials or featured customer stories with your permission.

We will not sell your information or information on your End Users to third parties so they can market their products to you or gain insights into you or your and your End User's preferences. We will not knowingly market to minors.

3.2 Our communication with you

We will communicate with you through the contact details you provide to us. You agree that we can communicate with you electronically. Our standard communication mechanisms include email, smart device notifications, SMS, web chat and telephony.

You can change your contact settings in your account. You can choose to opt-out of communications with respect to our promotion of third party products or services. You can opt out of our promotional communications using the unsubscribe link within our emails. You cannot opt-out of communications for Operational Purposes as these are fundamental to delivery of our Services.

24 HOW WE SHARE YOUR INFORMATION

4.1 Sharing with our related companies, partners and providers

We share information with related companies: As a global company we have a number of corporate entities which provide our Products. We may need to share your information among these related companies. We will do so only to support your use of our Products.

We share information with service partners: You may request Products that require us to direct you to third party providers such as Cyber Experts and third party providers technology and equipment. If so, we will need to share relevant information with these parties. We try to only be associated with reputable organisations and when we partner with them we require them to have privacy policies reasonably in line with ours. We cannot however be responsible for their information handling practices.

We use operational service providers: We work with third-party service providers to provide website and application development, hosting, maintenance, backup, storage, virtual infrastructure, payment processing, analysis customer, technical and sales support services. These services may require them to access or use information about you. If a service provider needs to access information about you to perform services on our behalf, they do so under instruction from us, including abiding by policies and procedures designed to protect your information.

We share information with resellers: We provide our Products through third party resellers such as telecommunications companies and technology vendors. If you have purchased our Products through such a third party then we will exchange information with them for the purpose of setting up your account, billing you and other Operational Purposes only.

We may provide links to third party sites and services: Our Products may contain links to websites owned or operated by third parties such as App Stores, Cyber Experts or others. Your use of sites and services any information you submit to them is governed by their privacy policies, not this one.

4.2 Sharing with other third parties

You may need to use App stores to access some of our Products: Where you acquire or download our Products from app stores or marketplaces (eg Google Play and Apple App Store) we will exchange limited information with them to support the app, extension or application's installation, update, support and operation. You will be required to agree terms including privacy terms with the relevant store or marketplace owner. The information you share with them is governed by their privacy policies, not this one.

We may share information with authentication providers: If you have enabled a "sign in with" service (eg through Google or Facebook) then we will exchange authentication information with them such as your name and email address. You will be required to accept their terms of use and policies with respect to the exchange of information. We will only use such services for the purpose of authentication.

We may offer you third party widgets: We may present you with social media widgets such as Facebook "like" or Twitter "tweet" buttons. We will not knowingly present these to minors. These widgets capture your IP address, the page you are visiting, and may set a cookie to enable the feature to function properly. Your interactions with these widgets is governed by the privacy policy of the company providing it.

4.3 Sharing for marketing purposes

We won't sell or provide your information for marketing purposes: We will not sell or provide your or your End User's personally identifiable information to third parties so they can market their products or services to you.

We may promote to you: We may contact you about our Products and offers or third party products or services which we reasonably consider to be complimentary or may be of interest to you. You can opt out receiving communications about third party products and you can unsubscribe to our marketing emails. While we try to work with reputable partners, we do not control their privacy practices and cannot be held responsible for their actions or omissions.

We will not market to children: We will not knowingly market to children.

4.4 Sharing between parents and schools

Where both a parent (account holder) and a school (account holder) opt-in to our school community feature then we will share information between them with respect to the relevant students. What information and how we share it is set out below in POLICY: SCHOOLS.

4.5 Sharing for Operational Purposes

We share limited information through hot-spots: When End Users connect to our networking Products (e.g., access points, network gateways) an authentication process will be triggered. Device and/or authorization tokens/certificates or a sign-in will allow our Services to identify an End-User (where possible). This is fundamental for the operation of our Services. Once registered, devices can be recognized by participating network gateways. We will share your End User's masked names (first name and first initial of last name) and device identification information where they connect to participating networks.

We share your name if you seek to adopt an End User: Should you request to 'adopt' an End User that has been previously registered to another account we will disclose your name to the primary parent of the subject End User. This is required to assist them to judge whether

the request should be granted. We are unable to enable (what we call) shared arrangements without this.

4.6 Other sharing with your consent

We may share specific information with your consent: We share information about you with third parties when you give us specific consent to do so. For example, testimonials.

We will share your submissions forums: If you choose to participate in a forum or comment in a blog or wiki provided by us, then the membership of the relevant resource will have access to your submissions. If the resource is public then your submissions will be public. We are not responsible for third party use of information submitted by you in either of these circumstances.

4.7 Exceptions

We may share information for Legitimate Business Reasons or for legal reasons: We reserve the right to disclose your information without your consent if we reasonably believe that access, use, preservation or disclosure of such information is reasonably necessary to:

(a) satisfy any applicable law, regulation, legal process, or governmental request;
(b) enforce applicable Customer Terms, including investigation of potential violations or breaches;
(c) detect, prevent, or otherwise address illegal or suspected illegal activities, security or technical issues; or
(d) protect against harm to the rights, property or safety of us, our users or the public as required or permitted by law.

We may share information as part of a business transfer: We may share or transfer information we collect under this policy in connection with any merger, sale of company assets, financing, or acquisition of all or a portion of our businesses to another company. You will be notified via email and/or a prominent notice if such an event takes place, as well as any choices you may have regarding your information.

25 HOW WE STORE AND SECURE INFORMATION WE COLLECT

5.1 Information storage

We use reputable data hosting service providers to host the information we collect, and we use technical measures to secure your data.

While we implement safeguards designed to protect your information, no security system is impenetrable and due to the inherent nature of the Internet, we cannot guarantee that data, during transmission through the Internet or while stored on our systems or otherwise in our care, is absolutely safe from intrusion by others. We will respond to requests about this within a reasonable timeframe.

5.2 International Privacy

We are a global provider. Where seek to store data we collect in the country associated with it. We call this “Regionalisation”. We regionalise the data we collect in relation to you End User’s use of our Products. Where possible we will regionalise other data we collect in relation to you or your End Users however this will not always be possible.

Accordingly we may transfer, process and store some of your information outside of your country of residence. We will only do so for the purpose of providing you the Products. Whenever we transfer your information we will take steps to protect it and we will capture, store and deal with it in accordance with this Policy.

Some of the third parties described in this policy, which provide services to us under contract, are based in countries other than yours. These other countries may not have equivalent privacy and data protection laws to the country in which you reside. Where we provide international third parties with your information we agree to take reasonable steps to ensure they use and manage it in a manner consistent with this policy.

5.3 Inter-company transfers

As a global company we have a number of corporate entities across the world which provide our Products. We need to share your information among these related companies. We will only do so in support of your use of our Products. Where our related companies access information about you, they do so under instruction from us, including abiding by policies and procedures designed to protect your information.

5.4 Our Security Procedures

We take information security seriously and have implemented a security program including administrative, technical, physical and managerial measures that is reasonably designed to protect the information we collect from loss, misuse and unauthorized access or disclosure. For example:

- ✓ We utilize Secure Sockets Layering to encrypt communication between us.
- ✓ We do not store your payment information. Instead we use a third PCI-DSS compliant party payment provider.
- ✓ We require you to provide a unique username and set a password and other security measures from time to time such as PINs.
- ✓ We hold passwords encrypted and cannot re-issue these (instead you must enter a new one).
- ✓ Where reasonable we pseudonymize your information, and in particular End User records.

5.5 Your Security Procedures

We urge you to be diligent in securing your computing networks, devices, usernames and passwords. Should other parties obtain access to these or guess them (because they are too simple) then your information may be compromised.

For convenience we make certain technologies available to you to make it easier to log in to your account or be authenticated to access the network or internet. For example, cookies, remember-me and single-sign-on type technologies. If you use these technologies, then we urge you to use device PINs and to log off your device when you're not using it.

If you intend to sell or return a device which you have used with us you should remove our application/s, log-out and clear the cache, all browsing information and cookies before doing so.

You are responsible for maintaining the confidentiality of your account access information and for restricting access to your computer or device through which a Family Zone account is accessed.

5.6 How long we keep information

We retain information to provide you with the services and features you have requested and to support the ongoing improvement of our Products. We take steps to secure and obfuscate your identity and once it's no longer needed, to de-identify your information or delete if.

How long we keep information we collect about you depends on the type of information collected.

- We will keep Personally Identifiable Information only for as long as it remains necessary for its identified purpose or as required by law, which may extend beyond the termination of our relationship with you.
- On cancellation of your account we will not automatically delete or de-identify the information we hold relating to you or your End Users. We need to retain some of your account information to comply with our legal obligations such as ensuring we're capable of resolving disputes, enforcing our agreements and collecting outstanding payments.
- There is some information we hold on you where for legal and Legitimate Business Reasons, we will not be able to delete, even if you request us to do so. For example, under taxation laws we need to maintain a record of your account and the financial transactions we've completed. We have obligations to retain information to ensure we're capable of resolving disputes, enforcing our agreements and collecting outstanding payments.
- When we delete information, we hold on you or your End Users, it may continue to be stored in backup archives. We will securely store such information and isolate it from any further use until deletion or de-identification is possible.
- If an End User associated with your account is also an End User in another account (eg a shared parenting arrangement of school student account) then deletion in your account will not automatically delete them in the other user's account.
- Our standard policy is to store Cyber Safety Data for 30 days. After that time related records are aggregated and anonymized. We MAY offer you the option to extend this storage period. For the purpose of quality assurance or due to technical limitations we may capture temporal Cyber Safety Data when Authorized End Users have set to be "not tracked". We will however purge such data as soon as practical.
- If you acquired our services through a Reseller cancellation of your account with us and requests for us to remove record of you will not automatically remove record of you in the reseller's platforms. This is because you were a customer of theirs.
- If you have elected to receive marketing emails from us, we retain information about your marketing preferences unless you specifically ask us to delete such information. We retain information derived from cookies and other tracking technologies for a reasonable period of time from the date such information was created.
- Notwithstanding the foregoing, Personally Identifiable Information stored by us, relating to End Users under the age of 18 will be deleted in all cases (to the extent that it is reasonably and commercially possible to do so) when it is no longer needed for the purpose for which it was collected.

26 HOW TO ACCESS AND CONTROL YOUR INFORMATION (YOUR OPTIONS)

You have a range of options available to you when it comes to your information. Below is a summary of those choices, how to exercise them and any limitations. We will respond to requests about this within a reasonable timeframe.

You have the right to request a copy of your information, to object to our use of your information (including for marketing purposes), to request the deletion or restriction of your information, or to request your information in a structured, electronic format.

Set out below are the tools and processes for making these requests. You can exercise some of your options in your account or through using our Products. Where the products are administered for you by another party (eg your parents or school) you will need to contact them to assist you. For all other requests, you may contact us as provided in the Contact Us section below to request assistance.

Your request and choices may be limited in certain cases: for example, if fulfilling your request would reveal information about another person, or if you ask to delete information which we or your administrator are permitted by law or have compelling legitimate interests to keep. Where you have asked us to share data with third parties, you will need to contact those third-party service providers directly to have your information deleted or otherwise restricted. If you have unresolved concerns, you may have the right to complain to a data protection authority in the country where you live, where you work or where you feel your rights were infringed.

(a) **Access and update your information:** You can access and modify the personal information about you in your account.

(b) **Delete End Users:** You can delete End Users from your account. Please note if the End User is also an End User in another account (eg a shared parenting arrangement of school student account) then deletion in your account will not automatically delete them in the other user's account.

(c) **Delete Avatars:** You can delete End User avatars from the Product you loaded it into.

(d) **Request that we stop using your information:** In some cases, you may ask us to stop accessing, storing, using and otherwise processing your information where you believe we don't have the appropriate rights to do so. For example, if you believe an account was created for you without your permission or you are no longer an active user, you can request that we delete your account as provided in this policy. Where you gave us consent to use your information for a limited purpose, you can contact us to withdraw that consent, but this will not affect any processing that has already taken place at the time. When you make such requests, we may need time to investigate and facilitate your request. If there is a delay or dispute as to whether we have the right to continue using your information, we will restrict any further use of your information until the request is honored or the dispute is resolved. If you object to information about you being shared with a third-party app, please disable the app.

(e) **Opt out of communications:** You may opt out of receiving third party promotional communications from us in your account. You may opt out of our promotions by using the unsubscribe link within each email. Even after you opt out from receiving promotional messages from us, you will continue to receive transactional messages from us regarding our Products. You can opt out of some notification messages in your account settings. You may be able to opt out of receiving personalized advertisements from other companies who are members of the Network Advertising Initiative or who subscribe to the Digital Advertising Alliance's Self-Regulatory Principles for Online Behavioral Advertising. For more information about this practice and to understand your options, please visit: http://www.aboutads.info, http://optout.networkadvertising.org/ and http://www.youronlinechoices.eu.

(f) **Turn off Cookie Controls:** Relevant browser-based cookie controls are described in our Cookies & Tracking Notice.

(g) **Send "Do Not Track" Signals:** Some browsers have incorporated "Do Not Track" (DNT) features that can send a signal to the websites you visit indicating you do not wish to be tracked. Because there is not yet a common understanding of how to interpret the DNT signal, our Services do not currently respond to browser DNT signals. You can use the range of other tools we provide to control data collection and use, including the ability to opt out of receiving marketing from us as described above.

(h) **Set End Users to "Do Not Track":** We offer you the ability to not track some Cyber Safety Data of End Users as a setting. This is described in section 2.

(i) **Data portability:** Data portability is the ability to obtain some of your information in a format you can move from one service provider to another (for instance, when you transfer your mobile phone number to another carrier). Should you request it, we will provide you with an electronic file of your basic account and End User information.

27 POLICY: ADVERTISING WITH THIRD PARTIES

We may from time to time use display advertising on the web and in platforms like Google and Facebook. Our advertising will only be aimed at supporting your engagement with cyber safety and education (such as topical information and insights) and maximizing what you get out of our Products (such as promoting features and events).

We will not knowingly market to minors.

You may have options in your browser or through the websites you access to limit or avoid advertising. You may also be able to opt out of personalized advertisements through the Network Advertising Initiative or Digital Advertising Alliance's Self-Regulatory Principles for Online Behavioral Advertising. For more information about this practice and to understand your options, please visit: http://www.aboutads.info, http://optout.networkadvertising.org/ and http://www.youronlinechoices.eu.

28 POLICY: DATA BREACHES

We are committed to transparency with respect to serious data breaches.

Where a data breach occurs which is likely to result in serious harm to any individuals whose personal information has been breached, then we will notify the relevant affected individuals (and other parties as required by law) and advise:

- ✓ Our identity and contact details;
- ✓ A description of the data breach;
- ✓ The kinds of information concerned; and
- ✓ Recommendations about the steps the individual should take in response to the data breach.

29 POLICY: SPAM

SPAM is a common term for unwanted commercial electronic messages including emails, short messages, etc. In various countries around the world there are laws designed to inhibit the use of SPAM by commercial organizations.

- ✓ We do not engage in SPAM;
- ✓ We will not use false, or misleading subjects or email addresses;
- ✓ We will identify marketing messages as such in a reasonable way;
- ✓ We will include our registered address;

- ✓ We will monitor Partner Marketing for compliance;
- ✓ We will honor opt-out/unsubscribe requests in reasonable timeframes; and
- ✓ We will provide opt-out unsubscribe options in relation to Partner Marketing.

210 POLICY: SCHOOLS

In this section of our Policy you/your refers Family Zone account holders that are Schools.

10.1 Our Commitment to Student Privacy

We are committed to complying with the Family Education Rights and Privacy Act ("FERPA") and the Children's Online Privacy Protection Act ("COPPA") in all applicable respects with regards to the collection, use, disclosure, and retention of the Personally Identifiable Information of minors. We have also taken the Student Privacy Pledge introduced by the Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA).

10.2 School Obligations

You may have different obligations to us with respect to privacy and in particular with respect to Student Information. We suggest you consult with your own legal counsel to ensure your compliance as we cannot take responsibility for your failure to comply with applicable laws or regulations.

10.3 Consent

Our Products can provide you with the ability to access, monitor and use information associated with Students and Staff (and guests accessing a network or devices running our Products). You are required to obtain and maintain all necessary consents with respect to your access, use and disclosure of such information.

10.4 Information we collect when we register Students and Staff

Where you register Students or a Staff in our Products we will also ask for information about their role in your school or class and for identifiers such as student IDs or student email addresses. If you require us to use third party services such as Google Education then we will also capture identifiers to permit us to interact with those third party services strictly only for the purposes of supporting your requirements such as user authentication.

10.5 School initiated Parent accounts

Our Products permit you to pre-register accounts on behalf of Parents. When using this feature, you are obliged to have or obtain consent from Parents before taking this action. Our Products allow you to:

(a) **Create inactive accounts:** This is where you provide us with the minimal sign up information (parent names and contacts, student names and dates of birth and device IDs for school provided devices). This method generates an activation email to the parents whom are then required to accept terms, to set up security settings and complete set-up.

(b) **Parent Referrals:** This is where we generate a special activation code which can be embedded in emails sent by us or the school to parent. Parents need only to follow the embedded link to obtain a custom set up process.

10.6 Advanced network filtering services

As a school we may offer you advanced cyber safety and security technology, not available to consumers. Such technology provides greater interception and inspection capability. For example, you choose to be able to view search terms used or messages travelling across the School network.

You are responsible for the efficacy and disclosure of your use of such services to affected parties.

Information collected by us using these advanced services is treated as Cyber Safety Data.

10.7 Marketing to Parents and Children

We will not directly market our Products or offers to Parents associated with your End Users without your permission unless we have permission from them or another valid source. We will not knowingly market to Students.

10.8 School community feature – School Access to Personal Student Data

Our Products can provide you with the ability to collaborate with parents in the management of student access to the internet and devices. We call this the school community feature and it allows schools to:

(a) Have access to the cyber safety data associated with students at the school, including data captured by us outside of school times and off the school owned network or devices.

(b) View information with respect to devices registered to the Student, including whether our on-device Products are installed and functioning.

(c) View the settings of parents which are in conflict with the school, such as setting a student to be in a rest-day when they're at school.

Collectively we call this 'personal student cyber safety data'.

Your access to personal student cyber safety data is subject to an opt-in by the relevant parents. Parents can revoke this at any time. Personal student cyber safety data is managed according to this policy and the choices of the relevant parents.

10.9 School community feature – School Access to School Data

Our school community feature also allows schools, subject to parent opt-in where applicable, to apply school internet access and device use policies to student devices during designated school times.

For the purpose of clarity, Cyber safety data collected during the application of school policies is owned by the school (not the associated parent) and is subject to our agreement with you.

10.10 School community feature – Parent Access

Our school community feature allows parents to access Cyber Safety Data owned by you in relation to their children (End Users). Such access requires the relevant parent to have an account with us and for both them and you to opt-in to the school community feature.

10.11 Extended storage of personally identifiable information

You may request us to extend the period within which we store personally identifiable information with respect to you or your End Users. For example, whilst our standard policy is to de-identify Cyber Safety Data at 30-days, you may request us to extend that timeframe.

Where you request us to do so, and we agree then:

(a) You acknowledge that you are responsible and agree to indemnify us and hold us harmless whatsoever, for any implications under relevant privacy laws in relation to the duration of storage of personally identifiable information; and

(b) You undertake to reflect your policy with respect to the duration of storage of personally identifiable information in your privacy policy and to communicate this to your End Users and their parents.

211 POLICY: COOKIES AND OTHER TRACKING TECHNOLOGIES

11.1 What types of technologies do we use?

We and our third party partners, such as our advertising and analytics partners, use various technologies to collect information, such as cookies and web beacons. In this notice we collectively describe these technologies as cookies.

We use cookies to improve and customize our Products and your experience; to allow you to access and use our Products without re-entering your username or password; to understand usage of our Products and the interests of our customers; to determine whether an email has been opened and acted upon; and to present you with information and advertising relevant to your interests.

11.2 How do we use cookies?

(a) **Where strictly necessary.** These cookies are essential. They enable our Products to function, for example remembering you are signed in.

(b) **For functionality.** These cookies remember choices you make such as language or search parameters. We use these cookies to provide you with an experience more appropriate with your selections.

(c) **For performance and analytics.** These cookies collect information on how users interact with our Products and enable us to improve how they operate. For example, we use Google Analytics cookies to help us understand how visitors arrive at and browse our products and website to identify areas for improvement such as navigation, user experience, and marketing campaigns.

(d) **Targeting Cookies or Advertising Cookies.** These cookies collect information about your browsing habits in order to make advertising relevant to you and your interests. They remember the websites you have visited and that information is shared with other parties such as advertising technology service providers and advertisers.

(e) **Social media cookies.** These cookies are used when you share information using a social media sharing button or "like" button on our websites or you link your account or engage with our content on or through a social media site. The social network will record that you have done this. This information may be linked to targeting/advertising activities.

11.3 How can you opt out?

To opt out of our use of cookies, you can instruct your browser, by changing its options, to stop accepting cookies or to prompt you before accepting a cookie from websites you visit. If you do not accept cookies, however, you may not get the best experience out of our Products.

Many browsers include their own management tools for removing HTML5 local storage objects.

Please visit familyzone.com/tracking for more information.

212 POLICY: LAW ENFORECEMENT REQUESTS

The following information is provided for law enforcement entities seeking information about our account holders and End Users.

All law enforcement requests for information should:

- Be directed to us at legal@family zone.com;
- Be written in English;
- Include all relevant identifiers to permit us to search our records;
- State specifically what information is being requested, why it's being requested and how it pertains to the investigation; and
- State the applicable act, law or ruling under which the law enforcement agency is requesting the data.

In the event of an emergency involving the danger of death or serious physical injury to a person please ensure the subject is: **Emergency Disclosure Request**.

We will respond to to valid, properly served legal process to the extent required by law.

It is our policy to use commercially reasonable efforts to notify affected account holders when we receive legal process requests for user data. Generally, except where a court order (and not just the request for information itself) requires delayed notification or no notification, or except where notification is otherwise prohibited by law or where we, in our sole discretion, believe that providing notice would be futile, ineffective or would create a risk of injury or bodily harm to an individual or group, or to our property, we will endeavour to provide reasonable prior notice to the relevant user of the request for user data in the event the user wishes to seek appropriate protective relief.

213 POLICY: DISCLOSURES OF HARM

13.1 Submissions via an End User

(a) The following policy relates to situations where an End User discloses to us information through a contact or feedback form and which indicates an incident or an intention to cause harm to themselves or others (a "Disclosure of Harm").

(b) For the purpose of clarity:

(i) We do not provide mental health, crisis, counselling, or support services. Where we receive a Disclosure of Harm, we will take reasonable steps as lay persons only;

(ii) Where a Disclosure of Harm is indicative of serious threat to life, health or safety of an individual then we reserve our rights to disclose such information to relevant authorities, schools and parents/guardians, subject to our obligations under relevant privacy legislation; and

(c) In the context of this clause 13:

(i) **Foreseeable:** means a future risk which can be reasonably predicted based upon a result of inferred actions, occurring as a result from a disclosure which indicates a method of harm, or a specified time, date, time-frame or location of harmful act.

(ii) **Imminent:** means a Disclosure of Harm indicative of a Foreseeable risk (as above), which requires immediate action, as inaction is likely to result in harmful activities.

(d) Where an End User discloses to us an Imminent and serious threat to life, health or safety then we will:

(i) Make reasonable steps to identify the End User, their School and their Parents (or guardians);

(ii) Make reasonable steps to contact the End User's School and Parents (or guardians) and provide a transcript of the Disclosure of Harm;

(iii) Contact the local police and request a welfare check.

(e) Where an End User otherwise discloses to us a serious threat to life, health or safety then we will:

(i) Make reasonable steps to identify the End User, their School and their Parents (or guardians);

(ii) Make reasonable steps to contact the End User's School and Parents (or guardians) and provide a transcript of the Disclosure of Harm;

(f) In all cases of Disclosures of Harm we will provide End Users with details of relevant support services.

13.2 Indications based on End User activity

(a) The following policy relates to situations where you have requested from us to activate services which permit us to monitor End User activity for the purpose of identifying risky behaviour ("Behavioural Insights").

(b) The services which support us providing you with Behavioural Insights may also identify behaviour indicative of self-harm.

(c) We do not promise or in any way undertake to monitor Behavioural Insights. Accordingly, we are unable to promise to escalate identified issues or risks of harm to you or relevant schools or authorities.

214 NOTICE TO END USERS

This notice is directed at End Users of our Products.

End Users are registered to account holders. You may have a primary account holder eg your parent or employer. You may also be

associated with other accounts such as where you are a party to a shared parenting arrangement or you're a student at a school using our Services or you're a guest on a network using our Services.

Account holders have the access to the information we hold on you and in particular the Cyber Safety Data related to you. This access is limited by and provided in accordance with this policy.

If you have queries with respect to the Products or your information, please direct your questions to the account holder/s administering you.

215 CHANGES TO THIS POLICY

We may, from time to time and in our sole discretion, make changes to this policy. We will provide notice to you by email (if you have provided us with one) or when you sign in to your account for the first time after the change.

We will ask you to review and agree to the changes. If you agree to the changes, simply continue using the Products (which will be deemed acceptance of the updated policy). If you object to any of the changes, immediately notify us at the contact information below.

18 HOW TO CONTACT US

If you have any questions about this Privacy Statement, the information that we collect from you or your End Users, or the Products, please contact us at privacy@familyzone.com.

You may also mail us at Privacy Officer, Family Zone Cyber Safety Limited 945 Wellington Street West Perth WA 6005, AUSTRALIA.