Linewize
BY FAMILY ZONE

Last Updated: **July, 2020**

Linewize **Privacy Policy**

1. Introduction

Our 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.

Your privacy is of critical importance to us. We collect and use data strictly in accordance with best practices and relevant laws. We collect the minimum information necessary and retain your data only for as long as is necessary to provide our services, or until you tell us to delete it. Your data is never sold or given to Third Parties.

If you do not agree with our policy, please do not access, or use our products.

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;
- Data associated with your use of our products is owned by us; and
- Data which cannot reasonably be attributed to you or an End-user (through anonymisation) is owned by us.

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

Our privacy policy sets out our agreement with you, the account holder and the owner of your information. If your account was created and/or paid for by another party (such as a school) then you are still the account holder and these arrangements are between you and us.

2. Our commitment to schools & student privacy

As a provider of cyber safety products to schools we act as a school official, operating under your direction and control. In this capacity, we have a legitimate educational interest in the collection, use, disclosure, and retention of information with respect to your students and staff.

2.1. School PII

In providing our products to schools we will collect personally identifiable information with respect to students, their parents and guardians and school staff (“School PII”).

You own the School PII provided to us.

Our privacy policies extend to any School PII collected by us, including that associated with school staff.

2.2. Our Commitment to Student and Staff 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 School PII.

We have also taken the Student Privacy Pledge introduced by the Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA).

Specifically, we will never sell, rent, or disclose School PII relating to students to third parties.

2.3. School Obligations & Consent

We acknowledge that as a school, you have various specific obligations with respect to privacy and in particular in relation to student PII. We need you to meet your obligations so we can meet ours. We require you to obtain and maintain all necessary consents with respect to your access, use and disclosure of School PII to us.

2.4. Information we collect when we register Students and Staff

When you register students or a staff for use of 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.

If you wish for us to communicate with the school community then we will capture names and contact details associated with your student's families.

We may capture other PII in relation to students where you specifically authorize us to do so.

2.5. Our commitment

We will capture, use, share and retain School PII in accordance with this privacy policy.

We limit access to PII to only those employees or subcontractors who require it for the purpose of providing our products to you. These employees and subcontractors will be trained on the application of our privacy policy.

We use PII to provide products to you. Other than with consent, we only disclose School PII to comply with the law or a court order, or a legal process, with a third party in the event we transfer our business, to protect the safety of users or others or the security of our site, and with our third party service providers solely to enable the provision of our products and services to you. If we share School PII pursuant to a court order or legal process, we will provide you with notice unless notice is expressly prohibited by law or court order. Our third-party providers will also not share or use your School PII for any other purpose except providing our products and will maintain reasonable security procedures and practices.

We will use School PII that has been de-identified to improve our products.

2.6. Cyber Safety Data

By default, we store school Cyber Safety Data for 12 months. You may request us to extend the period. Where you do so, and where we can do so, then:

- 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
- 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.

We may offer you advanced cyber safety and security technology, not available to personal account holders. Such technology provides greater interception and inspection capability.

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 in accordance with this privacy policy.

2.7. Review, Correction or Removal of Data

We only accept requests to review, change or remove PII from our main contacts with your and your identified administrators. Parents or legal guardians who request changes to or removal of your PII should go through you.

2.8. Marketing to Parents and Children

We will not directly market our products or offers to parents/guardians associated with your users without your permission unless we have permission from them or another valid source. We will not knowingly market to students or engage in targeted advertising. We will also not engage in targeted advertising on any site based on information we receive through our agreement. We will not use information gathered through our agreement to amass a profile about a student except in furtherance of the purposes of our agreement with you.

2.9. School Community

Our products permit you to refer parents / guardians to us to create personal accounts with us. When doing so, you are obliged to have or obtain consent from them before taking this action. To enable verification of these parent personal accounts and association of students we may seek permission from you to interface to school systems (or third party systems). Such access may be revoked by you at any time.

Our products provide you and the parents/guardians of your students to share information on school calendars and student use of and access to the internet and devices. We call this the School Community feature. Such data is considered by us Cyber Safety Data and is subject to our privacy policy.

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.

Sharing of safety data is subject to an opt-in by each party, which can be revoked at any time.

2.10. For Schools in New York

We confirm that we comply with the applicable state law and regulations, including Education Law section 2-d and its implementing regulations at Part 121, and the “bill of rights” required therein. We will train all employees with access to your data on the requirements of state and federal law governing the confidentiality of such data. We will require all subcontractors to comply with the terms of this Privacy Policy, including its terms on data breach.

2.11. For Schools in California

Our Agreement and this Privacy Policy meet the requirements under California Education Code § 49073.1 and all other applicable state privacy laws.

3. The information we collect

3.1. Account and user related information

Contacts: When you sign-up we will ask for information to establish an account including your name and contact details. If you are a company or business, we will ask you for your business and tax registration details.

Addresses: We do not typically seek your address however we may if you order a physical product; if you request on-site support; if we need to communicate to you in writing or if our payment provider requires your address, post code or zip for verification purposes.

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

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

Support: When you use our support channels we will capture the information you share with us through emails, support tickets, over the telephone or in online chat services.

Admin Users: When you sign up we will create an administrative user for your account. You may create additional administrative users. We will require their name and security information such as a password and PIN.

End-users: End-users are those persons that are affected by our products (e.g. authentication, filtering, device management). End-users may be students (at a school) guests on your network, your staff or you. When you register End-users we will ask for their name and we may ask for a PIN or password so we can provide custom access or features.

Credit Information: If you are a company or an unincorporated organization we may complete a credit review on you and source information available publicly or properly available for such purposes from credit reporting, law enforcement or government agencies.

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 authorization from you before doing so.

Submissions: We may provide opportunities for you or your users to post submissions in a forum, comments in a blog, or to complete surveys and forms. These services are inherently public, and we are not responsible for what is submitted or any third-party use of what has been submitted.

Sensitive Information: Unless permitted by law and requested by you or required by law, we will not deliberately record or use sensitive information. For the purpose of this policy sensitive information means

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.

3.2. Cyber Safety Data

Our products enable you to monitor and control the use of the internet and devices by end-users. This includes use of networks and devices not owned by you. Our products necessarily capture usage and device information. We call this Cyber Safety Data and it may include:

- **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.
- **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.
- **Device Location:** Geo-location information derived from GPS services available on smart devices.
- **Activities:** Actions taken or patterns of actions which are indicative of behaviour. For example, if an End-user installs or deletes an App. Such actions can be logged by us and made available to you.

3.3. System related information and analytics

Diagnostic Information: Our products log system level activities. We capture this information for quality assurance purposes only. It is stored for a short period of time.

Transactional records: 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.

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.

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.

Third party authentication services: For your convenience we may offer you or your End-users the ability to sign-in to our products using third party authentication services provided by organizations such as Google, Facebook or others. 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 authentica-

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

School information systems: For your convenience we may offer you the ability to interface our systems into school information systems (or integrators) for the purpose of enabling features such as enabling our systems to be aware of students and their schedules. Where you choose to enable our access, we will retrieve only the information necessary to perform services you've requested. Our access may be revoked by you at any time.

3.4. Privacy & Mobile Device Management

We use Apple Mobile Device Management ('MDM') in some of our products. MDM is a powerful tool which allows remote access to devices to monitor and control the functions available on them.

We use MDM for specific and limited purposes in the delivery of products to parents and schools (collectively 'you', 'your'). We only ever use MDM for the purposes of providing the products requested by you which may be:

- Scanning Apple devices for new Apps so we can notify you;
- Enabling or disabling access to device features such as the camera; screenshots; access to erotic content and so on; and
- Delivering a VPN profile to enable our web filtering services.

Account holders may disable any or all of these functions individually within their account.

Unless required by law or with your express consent, we will never sell or disclose any data collected by MDM to any 3rd party.

4. How we use your information

4.1. Our use of your data

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.

4.2. 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 repair;
- 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 purposes not listed above. For example, we may publish testimonials or featured customer stories with your permission.

We will not sell your information to third parties so they can market their products to you or gain insights into you or your and your end user's preferences.

5. How we share your information

In order to deliver to you the services requested and for us to meet our obligations we may from time to time share your information with others as described below.

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

Service partners: You may request products that require us to direct you to third party providers such as cyber safety experts and providers of technology and equipment. If so, we will need to share relevant information with them. We try to only work 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.

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. 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.

Resellers: We provide our products through third party resellers such as telecommunications compa-

nies and technology vendors. If you have purchased our products through a reseller then we will exchange information with them for the purpose of setting up your account, billing you and other operational purposes.

App stores: Where you acquire or download our products from app stores (e.g. Google Play, Google Web Store or 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 ours.

Authentication providers: If you have enabled a "sign in with" service (e.g. 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.

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.

Third party sites: Our products may contain links to websites owned or operated by third parties. Your use of sites and services and any information you submit to them is governed by their privacy policies, not ours.

Parents: Where both a parent (account holder) and a school (account holder) opt-in then we will share limited information between them with respect to relevant students. What information and how we share it is set out in this policy.

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 products to identify an end-user (where possible). This is fundamental for the operation of our products. Once registered, devices can be recognized by participating network gateways. We may share your end-users masked names (first name and first initial of last name) and device identification information where they connect to participating networks.

Shared end-users: Should you request to share cyber safety control of an end-user with another account holder then we will disclose your name to that other party. This is required to assist them to judge whether your request should be granted.

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

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.

Legal reasons: We may disclose your information without your consent if we reasonably believe that doing so is necessary to:

- satisfy any applicable law, regulation, legal process, or governmental request;
- enforce applicable Customer Terms, including investigation of potential violations or breaches;

- detect, prevent, or otherwise address illegal or suspected illegal activities, security or technical issues; or
- protect against harm to the rights, property or safety of us, our users or the public as required or permitted by law.

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.

6. How we store and secure your information

6.1. 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.

6.2. International Privacy

We are a global provider. We seek to store data in the country associated with it. We call this "regionalization". Where possible we will regionalize the 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 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 international third parties are in possession of your information, we will take reasonable steps to ensure they use and manage it in a manner consistent with this policy.

6.3. 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.

6.4. 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 an account is accessed.

6.5. 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 is no longer needed, to de-identify your information or delete it.

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

- We will keep information relating to you and your end-users 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. We retain de-identified information for as long as we consider necessary for our business purposes.
- On cancellation of your account we will not automatically (unless required by law) 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 which 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, 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 (e.g. a shared parenting arrangement or school student account) then deletion in your account will not automatically delete them in the other account.

- Our standard policy is to store Cyber Safety Data for 30 days on personal accounts and 12 months for school & business accounts. 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 even when end-users have set by you 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 records of you will not automatically remove records 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.

7. How to access and control your information

You have a range of options available to you when it comes to your information. Below is a summary of those choices. Where you request action from us, we will respond within a reasonable timeframe.

a. **Account information:** You can access and modify the information in your account.

b. **Delete End-users:** You can delete End-users from your account. Please note if the End-user is also in another account (e.g. a shared parenting arrangement or school student account) then deletion will automatically delete them in both accounts.

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.

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. You can opt out of some notification messages in your account.

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 disable tracking of some Cyber Safety Data in your account.

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.

j. **Requesting a copy of your information:** You may request a copy of information we hold on you. We will provide you with basic account level information without charge, Additional information may incur a reasonable charge. It may not be practical or proper to provide you some information (for example if fulfilling a request would reveal information about or owned by another party).

k. **Requesting deletion of your information:** You may request a deletion of information we hold on you. We will delete information where it is proper and practical to do so.

8. Data breaches

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

When 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.

Advertising & Marketing Policy

Advertising to minors

We will not knowingly market to minors.

Communications

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.

If you are a personal account holder then you can change your contact settings in your account.

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 if you opt-out of marketing or promotional communications you will continue to receive transactional messages from us.

PROMOTIONS

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 these communications. 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.

THIRD PARTY ADVERTISING

We will not sell or provide your information to third parties so they can market their products or services to you.

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).

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.

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.

COOKIES AND OTHER TRACKING TECHNOLOGIES

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. Specifically, 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. **For promotion.** These cookies permit us or a social media site to record that you have visited or used our products. We may use these to promote products we offer. We will not sell access to our cookies or use them for the purpose of promoting third party services to you.

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.

End User Policy

Law enforcement 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 valid, properly served legal processes 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.

Disclosures of harm

Submissions via an End-user
The following 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").

For the purpose of clarity:

- 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; and

- 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.

Disclosures of imminent and serious threat to life, health or safety
Where an End-user discloses to us an Imminent and serious threat to life, health or safety then we will:

- Seek to provide the End-user with details of relevant support services;
- Make reasonable steps to identify the End-user, their School and their Parents (or guardians);
- Make reasonable steps to contact the End-user's School and Parents (or guardians); and
- Contact the local police and request a welfare check.

In this context ***Imminent*** means a Disclosure of Harm indicative of a Foreseeable risk which requires immediate action, as inaction is likely to result in harmful activities and ***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.

Other disclosures of threats to life, health or safety
Where an End-user otherwise discloses to us a serious threat to life, health or safety then we will:

- Seek to provide the End-user with details of relevant support services;
- Make reasonable steps to identify the End-user, their School and their Parents (or guardians); and
- Make reasonable steps to contact the End-user's School and Parents (or guardians).

Indications based on End-user activity
We may offer you features of our products which monitor End-user activity for the purpose of identifying risky behaviour ("Behavioural Insights"). Such features may identify behaviour indicative of self-harm.

We do not promise that these Behavioural Insights are complete or accurate. We do not promise to monitor them or escalate issues to you or relevant authorities.

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 e.g. 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.

Changes to **our policies**

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.

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@linewize.com.

You may also mail us at Privacy Officer

Linewize USA, 11545 West Bernardo Ct, San Diego CA, United States.

Linewize Australia, Level 3, 45 St George's Terrace Perth WA Australia.