SEPTEMBER 2024 - V5.0

Qoria Privacy Policy

qoria.com

Qoria

Introduction

Our agreement

Our business involves advertising, marketing and the provision of digital safety technology, content and advice (our "Products") to you (the "account holder") and the persons associated with your account (the "End-Users"). We provide Products under an agreement with you (the "Customer Terms" which is accessible on our website) and our Customer Policies, which include this Privacy Policy.

Our Privacy Policy applies whether you have purchased Products from us directly or through resellers and if you download and use our Products.

In addition to this Privacy Policy we comply with relevant privacy and data protection regulations across the world and we voluntarily sign-up to various pledges, data protection agreements and the like. These are outlined below.

If you do not accept our privacy policy then you should not use our Products.

Information and ownership

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

This Privacy Policy describes how we collect, store, use and distribute this information. It also sets 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 Products, or until you tell us to delete it. Your data is never sold to third parties.

With respect the information we collect, generally speaking:

- 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 de-identification) 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.

End Users and consent

Our Products may be used by you to monitor and filter the activity of End Users such as students (at a school), your children, guests on your network, your staff or you.

We provide our Products to you under our agreement with you. You are responsible for informing your End Users and obtaining necessary consents from them or their parents/guardians with respect to the application of our Products and with respect to our collection, use and disclosure of information associated with them in accordance with this Privacy Policy.

Privacy & Schools

In providing our Products to school clients we will collect personally identifiable information with respect to students, their parents and guardians and school staff ("School Data"). We appreciate that schools have unique circumstances and specific obligations with respect to privacy and in particular in relation to information associated with students. If you are a school account holder, this section applies to you.

For schools in the United States

Our role in USA schools
As a provider of digital safety products to schools in the United States 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.

Regulations & pledges
We are committed to complying with the Family Education Rights and Privacy Act ("FERPA"), the Children's Online Privacy Protection Act ("COPPA") and the UK/EU General Data Protection Regulations ("GDPR") in all applicable respects with regards to the collection, use, disclosure, and retention of School PII.

Qoria participates in the iKeepSafe Safe Harbor program. Qoria School products (Monitor, Pulse, School Manager and Classwize) have been granted the iKeepSafe COPPA Safe Harbor seal signifying approval for having policies, security and practices surrounding the collection, use, maintenance and disclosure of Personal Information from children that meet the requirements of the iKeepSafe COPPA Safe Harbor program. If you have any questions, please do not hesitate to contact privacy@qoria.com or the iKeepSafe Safe Harbor program at COPPAprivacy@ikeepsafe.org.

Qoria School products (Monitor, Pulse, School Manager and Classwize) hold the iKeepSafe FERPA Certification signifying approval for having policies, security and practices that are compliant with the federal mandates for FERPA.

Qoria also maintains the California Student Privacy Certification (CSPC) issued by iKeepSafe.

The certification assesses for federal and California laws governing student data privacy, including:

- Family Educational Rights and Privacy Act ("FERPA")
- Protection of Pupil Rights Amendment ("PPRA")
- California Education Code 49073.6 – Collection of Student Information from Social Media
- California AB 1584, Education Code section 49073.1 – Privacy of Pupil Records: 3rd-Party Digital
- Storage & Education Software
- Student Online Personal Information Protection Act ("SOPIPA")

The iKeepSafe certifications assert that your technology company is a leader in student privacy. These certifications help educators and parents find products that are assessed to meet the expectations of federal privacy laws.

Qoria is a proud signatory of the Student Privacy Pledge introduced by the Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA), agreeing to a set of principles intended to safeguard student privacy regarding the collection, maintenance, and use of student personal information.

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.

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.

Privacy & Schools cont.

For schools in the United Kingdom and European Union

Our role in UK and EU schools
For customers within the United Kingdom and the European Union, with respect to the GDPR, we act in the capacity of a data processor and you are the data controller with respect to any data captured, used and disclosed by us. These terms are defined in GDPR.

Other specific terms for schools

Consents from parents, students and staff
On your behalf we monitor, filter activity and capture, use and disclose School Data with respect to your End Users. We require you to obtain and maintain all necessary consents from these parties, in accordance with your local regulations (e.g. as required by COPPA in the US).

Extended data storage
By default, we store school Digital safety Data for 15 months however you may request us to extend that 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.

Safety & security incidents
You may subscribe to advanced digital safety and security technology from us which monitors End-User activity for the purpose of identifying or recording concerning activity. 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 Digital safety Data in accordance with this privacy policy. Where disclosures of harm are identified our End User Policy applies.

Marketing to parents and children
We will not directly market our Products or offers to parents/guardians associated with your End-Users without your permission unless we have permission from them or another legitimate 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.

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

School community Products
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. 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, Digital 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.

Messaging services for schools
Our Products permit the exchange of messages between End Users eg between teachers and students. Messaging services are provided under our arrangement with you (the “account holder”). You are required to obtain and maintain required parental/guardian consent.

Unless agreed with you otherwise:

- Users cannot delete messaging content. We will retain messaging content under the same arrangements agreed with you for Digital safety Data or otherwise as agreed with you or until you ask us to delete it.
- Messaging content exchanged between students and teachers is private to the student and you. We will not share it with other End Users or other parties (eg parents) unless permitted by you

Student Monitoring
Our products permit schools to monitor student advice and online activity. Where we reasonably can we will only capture information associated with activity which our products determine to be of a nature requiring escalation to moderators or school safety leads. Furthermore, we attempt but cannot promise to avoid capture of information unrelated to identified concerns such as personal data.

Where you enable monitoring you are responsible for the efficacy and disclosure of their use to affected parties. Information collected by us using these advanced services is treated as Cyber Safety Data in accordance with this privacy policy. Where disclosures of harm are identified our End User Policy applies.

Privacy & Personal Accounts

In providing our Products to parents & guardians (personal accounts) we will collect personally identifiable information with respect to account holders and End-Users being users of devices or home networks where our Products are installed.

If you are a personal account holder, please see the specific privacy policy **https://www.qustodio.com/en/family/privacy/.**

School community
Our Products permit parents and schools to collaborate and share information with respect to student activity. We call this the School Community feature. Such data is considered by us Digital safety Data and is subject to our privacy policy.

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

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

Disclosures of harm
Our Products may from time to time identify concerning activity. Where disclosures of harm are identified our End User Policy applies.

Data associated with Student Protection

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.

Device Usage: Logs of device activity including apps and features used, networks accessed and screen captures.

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.

Events: 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.

Incidents: Records of identified incidents detected by our Products or recorded by you or your end-users.

Calendars: Records of school and student schedules collected to support teachers to manage classroom activity.

Data associated with Student Monitoring

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.

Device Usage: Logs of device activity including apps used, keystrokes entered, features used, networks accessed and screen captures.

Cloud Services: Logs of concerning activity or media found by our services scanning your cloud services.

Data associated with Student and Teacher Wellbeing

Check-Ins: Our Products allow you to optionally enable check-ins where for example students or teachers may be asked how they are feeling and whether they would like some support.

Wellbeing indicators: Our Products allow you to optionally enable anonymised wellbeing questions to be asked of students to help schools identify cohort trends or concerns in wellbeing.

Educator data: Our Products allow schools to seek out feedback on educator wellbeing and if enabled we will capture limited information (e.g. first name, last name, email address and the year-groups taught) for the purpose of providing personalised 360-degree feedback, professional development resources, and professional development plans.

The Information We Collect cont.

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 a 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.

Please note that for Linewize by Qoria use and transfer to any other app of information received from Google APIs will adhere to Google API Services User Data Policy, including the Limited Use requirements.

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), your children, guests on your network, your staff or you.

- Consumer accounts: Please see the specific privacy policy https://www.qustodio.com/en/family/privacy
- School accounts: Where school institutions register End Users we will also ask for information about their role in the school, groups they are part of (e.g. class), classroom schedules and for identifiers such as student IDs or email address. If the school uses third party authentication services such as Google for Education then we will also capture identifiers to permit us to interact with those services but strictly only for the purposes of supporting your requirements.

Credit Information: If you are a company or an unincorporated organisation 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 authorisation from you before doing so.

School communities: We work with schools and businesses to provide digital safety Products to them and their communities. These organisations may refer us to parents/guardians or refer parents/guardians to us by providing us with relevant contact & student details. We require these parties to confirm to us that they have permission or a right under law to do this.

Submissions: We may provide opportunities for you or your End-Users to post submissions in a forum, comments in a blog, or to complete surveys and forms. We are not responsible for what is submitted or for monitoring or escalating concerning submissions. If submitted into a public forum we are not responsible for 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.

Digital 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 Digital 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.
- Events: 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.
- Incidents: Records of identified incidents detected by our Products or recorded by you or your End-Users.
- Calendars: Records of school and student schedules collected to support teachers to manage classroom activity.

The Information We Collect cont.

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 organisations, 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 pseudonymised. 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 third party providers, such as Google. Where possible we will provide at qoria.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 recognise 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 qoria.com/tracking.

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 organisations 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.

Messaging data

We may make available to you Products which permit the exchange of messages between End Users. Such messaging services are provided to and under our arrangements with you (the account holder). These arrangements include terms for whom can interact and the monitoring and retaining of message content. We are not responsible for the content submitted. If an End User on your account is enrolled in a school institution that is a client of ours then their messaging services will be managed under our agreement with that school institution.

Wellbeing data

Our Products may collect information about a student's wellbeing. For example, we ask you "How are you feeling today?" and questions about experiences at school. We use this data to help schools provide students with support they need when needed. For educators we obtain personal and demographic information (e.g. first name, last name, email address and the year-groups taught) this data is used for the purpose of providing personalised 360-degree feedback, professional development resources, and professional development plans. We also collect and store students' and other teachers' observations about participants' teaching practice, and calculate aggregate statistics to ensure that the feedback provided to participants is based on sound data.

Privacy & mobile device management

We use Mobile Device Management ('MDM') in some of our Products. MDM is a 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 devices for new Apps so we can notify you;
- Enabling or disabling access to device features such as the camera; screenshots; access to adult 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 or on the relevant device. Unless required by law or with your express consent, we will never sell or disclose any data collected by MDM to any third party.

The Information We Collect cont.

Purposes for processing your data

The table set out below identifies the data we collect, the purpose for which it is collected and our basis for doing so.

Purpose	Data collected	Legitimate interest or basis for doing so
To register you as a new customer, bill you and support your use of our services	Contacts, Addresses, Timezone, Payment Method	So we can perform in our agreement with you.
To communicate with or seek feedback from you with respect to our services and policies	Contacts, Addresses, Submissions, Support	So we can perform in our agreement with you. So we can comply with relevant legal obligations (eg notifications). So we can keep our records updated and to monitor and improve our services.
To deliver, support, secure and administer our services	Contacts, Addresses, Timezone, Support, Admin user, End user, Digital safety data, Messaging Data, Wellbeing Data, Diagnostic information, Web Analytics, Cookies and other Tracking Technologies, Third party authentication services.	So we can deliver services in accordance with our agreement with you. So we can comply with relevant legal obligations (eg data and security).
To provide a website which provides information on our services	Web Analytics, Cookies and other Tracking Technologies	So we can analyse our website activity to tailor it to what is of more interest to users. Because you consent to us capturing this.
To notify you of changes to and new services that may be of interest to you	Contacts, Digital safety data Web Analytics, Cookies and other Tracking Technologies	So we can deliver services in accordance with our agreement with you, improve our services, offerings and relationship with you. Because you consent to us doing this.
To assess your creditworthiness	Credit Information	So we can assess whether we may offer you commercial credit.

How We Share Your Information

In order to deliver to you the Products 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. All of our corporate entities and staff operate under the same internal policies, procedures and standards which enforce the level of protection for your data reflected in this policy.

Service partners: You may request Products that require us to direct you to third party providers such as digital safety experts, counsellors and providers of technology and equipment. If so, we will need to share relevant information with them. We only work with reputable organisations and when we partner with them, we subject them to checks which require them to have appropriate standards in place to manage your data. We encourage you to read their privacy policies and ensure you are fully informed.

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. A list of our sub-processors can be provided on request.

Resellers: We provide our Products through third party resellers such as telecommunications companies 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 End-User name and email address. You and your End-Users will be required to accept their terms of use and policies with respect to the exchange of information.

Learning system providers: If you have subscribed to learning Products provided by us then we will exchange limited information with our chosen learning management system such as end-user name, email address and group (e.g. class).

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.

Schools & parents: Where both a parent/guardian (account holder) and a school (account holder) opt-in then we will share chosen sets of Digital safety Data between them with respect to relevant students.

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 authorisation 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 recognised by participating network gateways.

Shared End Users: Should you request to share Digital safety Data associated with or 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 determine whether your request should be granted.

How We Share Your Information

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, End Users or the public as required or permitted by law.

If we share School Data pursuant to a court order or legal process, we will provide you with notice unless notice is expressly prohibited by law or court order.

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.

International privacy

We are a global provider. We seek to store data in the country associated with the account holder however this is not always practicable. Accordingly, we may transfer, process and store some of your information outside of your country. 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.

To ensure that your data is protected and transferred in a manner consistent with legal requirements:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data; and
- Where applicable, we may use specific contracts which give personal data an appropriate level of protection;

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data.

How We Secure Your Information

Information storage

We use reputable data hosting service providers (such as Google, Microsoft and Amazon Web Services) 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.

Our security procedures

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

- Choose to exclusively use Tier 1 data centers provided by Microsoft, Amazon and Google. These data centers facilitate us deploying security and resilience of the highest order.
- Encrypt your data in transit and at rest when stored in the data center using industry standard secure encryption technologies.
- Do not store your payment information. Instead we use a third PCI-DSS compliant party payment provider.
- Require you to provide a unique username and set a password and other security measures from time to time such as PINs.
- Hold passwords encrypted and do not re-issue them (instead you must enter a new one).
- De-identify your information where possible, and in particular End User records.

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.

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 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 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.

How We Secure Your Information cont.

How long we keep information

- Our standard policy is to store Digital safety Data for 30 days on personal accounts and 15 months for school & business accounts. After that time related records are aggregated and de-identified. We may offer you the option to extend this storage period.
- Unless otherwise agreed with you Messaging Data is stored for 12 months and will be deleted earlier if our contract with you ends.
- For the purpose of quality assurance, or due to technical limitations we may capture temporal Digital safety Data even when End Users have been set by you to be “not tracked”. We will however purge such data as soon as practicable.
- If you acquired our Products 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.

Your Rights

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.

Access

You can access and modify the information in your account at any time, this includes all data that is required to provide the Products.

Rectification

You can access and modify the information in your account at any time.

Relevant browser-based cookie controls are described in our Cookies & Tracking Notice. 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.

We offer you the ability to disable tracking of some Digital safety Data in your account.

Erasure

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 in your account will not automatically delete them in the other account. You can delete End User avatars from the Product you loaded it into.

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.

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

Restriction

Restriction is the right to stop further processing of your data, this will not affect any processing that has already taken place at the time but will suspend any further processing until the dispute is resolved.

Portability

Data portability is the ability to obtain 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 account and End User information. 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).

Objection

If there is a concern with regard to how we are storing, using, transferring, processing or treating your data you can contact us to raise that concern, 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.

However, we may be entitled to continue processing your information based on our legitimate interests or where this is relevant to legal claims.

Your Rights cont.

Withdrawal of consent

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.

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.

Complaints to the regulator

You also have a right to lodge a complaint with a supervisory authority, where you are located, where we are based or where an alleged infringement of Data Protection law has taken place.

Your contact options are set out to below:

United Kingdom
Office of the Information Commissioner
https://ico.org.uk/make-a-complaint/

Australia
Office of the Australian Information Commissioner
https://www.oaic.gov.au/privacy/privacy-complaints

New Zealand
Office of the Privacy Commissioner
https://www.privacy.org.nz/your-rights/making-a-complaint/

United States
Each state has its own relevant body.
https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy

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.

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 our Privacy & Data Protection Officer as follows:

Contacts

For customers within the Australia and New Zealand

e: privacy@qoria.com
m: Qoria Limited, Level 3, 45 St Georges Terrace, Perth WA 6000, AUSTRALIA.
p: +61 1300 687 052

For customers within the United Kingdom:

e: privacy@qoria.com
m: Second Floor, 2 Whitehall Quay, Leeds LS1 4HR, United Kingdom
p: +44(0)113 539 7506

For customers within the United States

e: privacy@qoria.com
m: 10803 Thornmint Rd. San Diego, CA 92127 USA
p: +844 SAFEWEB (844-723-3932)

Changes to our customer 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.

Qoria

Contact

e: enquiries@qoria.com

Global headquarters
Qoria Limited
Level 3, 45 St Georges Terrace,
Perth WA 6000, Australia.

qoria.com