



Qoria Privacy Policy

End User





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@Qoria.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 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.



Contact

e: enquiries@qoria.com

Global headquarters

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

qoria.com