



Privacy Policy

Apptrade's commitment to publishers and token holders.

Apptrade keeps all proprietary information confidential. We do not share ideas, analytics, or business strategies with other participants. Apptrade and all future virtual goods management firms and app portfolios are prohibited from altering or manipulating metadata displayed in any marketplace's dashboards. All data is measured fairly and is completely algorithmic.

All metrics for gauging the monetary value are held to a universal standard. Developers cannot buy their way to the top of featured portfolios. The order of all portfolios that appear on our site are displayed by categories. Users browse for app portfolios by editing search filters and parameters. Portfolio's potential value can be based on raw analytics and other immeasurable factors. All Apps in a portfolio are marketed together, however, when outliers appear, the portfolio may temporarily consolidate efforts behind select brands.

Apptrade views privileged internal app trends as a potentially unfair and fraudulent area of abuse. Apptrade avoids disclosing information to any exclusive group of buyers about apps yet to be listed. Apptrade and all app brokerages will not copy, reskin, or reverse engineer any submitted app unless given permission from the owner of the app. The 24 month distributor agreement for app publishers is currently the standard agreement for this distribution model. Developers may share information amongst each other on Apptrade dashboards. However, Apptrade is not responsible for the dynamics involved between developers that may find each other on the platform.

Sponsors, 3rd party buyers, and brokers are prohibited from transacting outside of the Apptrade platform and from sharing information about what they see on their respective dashboards. The point of this agreement is for the licensee to be the primary and exclusive representative across the digital goods marketplaces and the universe. We want to be the representatives involved in facilitating and curating offers for the acquisition of digital goods.

Laundering money, funding unlawful organizations or activities, or transferring illegal transactions through our platform is prohibited. Using apps as a conduit for masking the exchange of capital for illegal activity such as drugs, arms, human trafficking, smuggling, or terrorism will not be tolerated. Appttrade does its best to carry out due diligence to ascertain who is buying apps or tokens. It is up to the developer community to also keep an eye out for unlawful activity and report it to Appttrade.

Countermeasures to reduce these scenario include:

- All token reserves maintain a whitelist of accounts. Bad actors are rooted out quickly. To benefit from any app portfolio's buyback program participants must maintain their status on the whitelist.
- Beyond the token, Appttrade has a validation process that requests vital criteria and items to be delivered upon signup. Anyone can shop around, but token buyers will have to be verified.
- A unified standard for buying and selling is in place to build trust amongst developers and sponsors. Appttrade keeps key information about user data that is guarded at all times.

Privacy Policy Q&A

What personal information does Appttrade collect from users visiting site the site?

When ordering or registering on Appttrade, as appropriate, users may be asked to enter their name, email address, mailing address, phone number or other details to help with user experience. If at any time users would like to unsubscribe from receiving future emails, a user can typically follow instructions at the bottom of their email address.

How does Appttrade handle user information?

We may use the information we collect from you when you register, make a purchase, sign up for our newsletter, respond to a survey or marketing communication, surf the website, or use certain other site features in the following ways:

- To personalize general user experience and to allow Appttrade to deliver information about other participants.
- To follow up after correspondence (live chat, email or phone inquiries)

How do we protect user information?

Aptrade's site is scanned on a regular basis for security holes, known vulnerabilities, and potential threats in order to make site usership as safe as possible.

We use regular Malware Scanning.

Personal information is contained behind secured networks and is only accessible by a limited number of people who have special access rights to such systems, and are required to keep the information confidential. In addition, all sensitive/credit information you supply is encrypted via Secure Socket Layer (SSL) technology. We implement a variety of security measures when a user places an order enters, submits, or accesses their information to maintain the safety of personal information.

Do we use 'cookies'?

No, because we have no interest in commercialising your data.

Third-party disclosure

We do not sell, trade, or otherwise transfer to outside parties your personally identifiable Information or data.

Third-party links

Occasionally, at our discretion, we may include or offer third-party products or services on our website. These third-party sites have separate and independent privacy policies. We therefore have no responsibility or liability for the content and activities of these linked sites. Nonetheless, we seek to protect the integrity of our site and welcome any feedback about these sites.

California Online Privacy Protection Act

CalOPPA is the first state law in the nation to require commercial websites and online services to post a privacy policy. The law's reach stretches well beyond California to require any person or company in the United States (and conceivably the world) that operates websites collecting Personally Identifiable Information from California

consumers to post a conspicuous privacy policy on its website stating exactly the information being collected and those individuals or companies with whom it is being shared. <http://consumercal.org/california-online-privacy-protection-act-caloppa/#sthash.0FdRbT51.dpuf>

According to CalOPPA, we agree to the following: Users can visit our site anonymously, however, will be verified upon purchasing tokens or submitting content for listing. You will be notified of any Privacy Policy changes via our internal dashboards, a notice on the homepage, and the privacy policy page. Aptrade does not allow third-party behavioral tracking

COPPA (Children Online Privacy Protection Act)

When it comes to the collection of personal information from children under the age of 13 years old, the Children's Online Privacy Protection Act (COPPA) puts parents in control. The Federal Trade Commission, United States' consumer protection agency, enforces the COPPA Rule, which spells out what operators of websites and online services must do to protect children's privacy and safety online. Aptrade does not specifically market to children under the age of 13 years old.

Fair Information Practices

The Fair Information Practices Principles form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information. In order to be in line with Fair Information Practices we will take the following responsive action, should a data breach occur, we will notify you via email Within 1 business day.

Aptrade adheres to the Individual Redress Principle which requires that individuals have the right to legally pursue enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable rights against data users, but also that individuals have recourse to courts or government agencies to investigate and/or prosecute non-compliance by data processors.

CAN-SPAM Act

The CAN-SPAM Act is a law that sets the rules for commercial email, establishes

requirements for commercial messages, gives recipients the right to have emails stopped from being sent to them. Apptrade collects user email addresses in order to send information, respond to inquiries, and for other requests or questions

To be in accordance with CAN-SPAM, Apptrade agree to the following:

- Not use false or misleading subjects or email addresses.
- Identify the message as an advertisement in some reasonable way.
- Include the physical address of our business or site headquarters.
- Monitor third-party email marketing services for compliance, if one is used.
- Honor opt-out/unsubscribe requests quickly.
- Allow users to unsubscribe by using the link at the bottom of each email.



**Info @ [Apptrade.io](mailto:Info@Apptrade.io)
Last edited on 2017-01-29**