

Privacy Policy

How Universal Quantum collects, uses and protects your information.

DOCUMENT	EFFECTIVE	VERSION	ISSUED BY
Privacy Policy	July 2026	v2026.1	Universal Quantum

This Privacy Policy explains what personal data Universal Quantum ("we", "us", "our") collects when you visit the Platform or open an investor account, why we collect it, how we use it, who we share it with, how long we keep it, and the rights you have over it. It applies to every part of the Platform, including the marketing website, the investor dashboard and the administrative console. If you do not agree with anything in this policy, please do not use the Platform.

1. Who we are

Universal Quantum operates the Platform and is the controller of the personal data described in this Policy. Where a data-protection regime applies to your relationship with us, the controller is Universal Quantum unless we tell you otherwise for a specific processing activity. If you need to contact us about anything in this document, use the details in the **Contact** section at the end.

2. Scope of this policy

This Policy covers the personal data we handle in connection with the Platform. It does not cover the practices of any third-party website, application or provider that links to or from the Platform. Third parties have their own privacy notices; please read those before providing them with your data.

3. What data we collect

We collect data in the following categories:

- **Account data** — the name, email address, phone number (optional) and password hash you supply at registration, plus your Account preferences and history.
- **Identity data** — for KYC we may collect your full legal name, country of residence, government-issued identity document type and number and, where risk requires, source-of-funds documentation.
- **Financial and transaction data** — deposits (including TXIDs, coin type and network), the plans you take, your Available Balance, withdrawal history, referrals and reward activity.
- **Support data** — the content of tickets you open, replies you send, and messages posted through the contact form or live chat.
- **Technical data** — session identifiers, cookies, device information, IP address, browser type, operating system and language preference.
- **Preference data** — theme, layout, language and other display settings you choose, saved locally in your browser storage and, in some cases, in your Account.

4. Sources of data

We collect most of your data directly from you when you register, verify your identity, deposit or withdraw, contact support, or interact with the Platform. Some data (for example on-chain transaction confirmations and market rates) is obtained from public blockchain sources and reputable market-data providers. Technical data is captured automatically when your browser loads the Platform.

5. How we use your data

We use your data to:

- create and secure your Account, and authenticate you at each visit;
- process deposits, activate Investment Plans, record daily returns and settle withdrawals;
- verify your identity and meet our AML, sanctions and reporting obligations;
- detect, investigate and prevent fraud, abuse and unauthorised access;
- send transactional notifications (welcome, deposit confirmation, withdrawal paid, KYC decision, support replies, security alerts, password reset) and, where you have opted in, optional announcements;
- improve the Platform, its stability and its user experience;
- comply with legal, tax, regulatory and accounting requirements.

6. Legal bases

Depending on the activity, and where a regime such as the GDPR applies, we rely on one or more of the following legal bases: performance of a contract with you; compliance with a legal obligation; our legitimate interests (for example, operating a safe and viable platform, preventing fraud, and defending our rights); and, where required, your consent (for example, non-essential cookies or optional marketing). Where we rely on consent, you may withdraw it at any time without affecting the lawfulness of processing carried out before withdrawal.

7. Who we share it with

We do not sell your personal data. We may share limited data with:

- **Service providers** that help us operate the Platform (for example transactional email delivery, hosting, live-chat, translation, and on-chain data providers) and that are contractually bound to protect your data and to process it only on our instructions.
- **Authorities, regulators and law-enforcement agencies** where we are required to do so by law, court order, or a valid regulatory request.
- **Professional advisers** (for example legal counsel or auditors) bound by duties of confidentiality.
- **Successors in interest** if the Platform is reorganised, sold or merged, subject to the receiving party continuing to protect your data on comparable terms.

8. International transfers

Data may be processed in countries other than the one in which you live. Where a data-protection framework restricts international transfers, we take reasonable steps to ensure that the transfer is lawful — for example by using standard contractual clauses or an equivalent safeguard — and that your data continues to be protected to an equivalent standard.

9. 9. Retention

We keep your data only for as long as we need it for the purposes described in this Policy. Account and transaction records are typically retained for the period required by financial-services and AML regulations, which can be several years after Account closure. Support tickets are retained for as long as needed to give context to future issues. Technical logs are retained for a shorter period unless required for a security investigation. When data is no longer needed, it is deleted or securely anonymised.

10. 10. Data security

We apply industry-standard safeguards to protect your data. Passwords are stored using strong, one-way hashing (bcrypt); sessions are protected by HTTP-only, SameSite cookies over TLS; access to production systems is restricted to authorised staff and audited; and we monitor for anomalous activity. Deposit wallet addresses are configured by administrators only, and admin actions are logged to an audit trail.

No system is perfectly secure. Please protect your own credentials, enable two-factor authentication where offered, be alert to phishing, and never share your password or wallet keys with anyone — including anyone claiming to be from our team. We will never ask for them.

11. 11. Your rights

Subject to the applicable law in your country, you may have the right to:

- ask what personal data we hold about you and receive a copy of it;
- ask us to correct data that is inaccurate or incomplete;
- ask us to delete your personal data, subject to our legal and regulatory retention obligations;
- ask us to restrict or object to certain processing;
- ask for your data to be transferred to another controller in a structured, commonly used format;
- withdraw any consent you have given for optional processing;
- lodge a complaint with a supervisory authority in your jurisdiction.

To exercise any of these rights, contact us using the details below. We may need to verify your identity before we act, so that we do not release your data to the wrong person.

12. 12. Cookies & similar technologies

We use cookies and similar browser technologies to keep you signed in, remember your preferences and understand aggregate usage. Full detail — including the specific cookies used and how to manage them — is in our [Cookie Policy](#).

13. 13. Marketing & communications

You will receive transactional emails and in-app notifications because they are necessary to run your Account. We do not use your data for behavioural advertising, we do not build cross-site tracking profiles, and we do not share your data with ad networks. Any optional announcements are limited, relevant and easy to opt out of.

14. 14. Children

The Platform is not intended for anyone under eighteen (18) years of age, and we do not knowingly collect personal data from minors. If you believe a minor has provided us with personal data, contact us and we will take reasonable steps to delete it.

15. 15. Automated decisions

We may use automated tools to score risk (for example, to flag unusual transaction patterns for review). These tools inform our decisions but do not make binding decisions about you on their own — a human reviewer always makes the final call for consequential outcomes such as declining a withdrawal or closing an Account.

16. 16. Third-party links

The Platform may link to external websites (for example blockchain explorers, live-chat providers or educational articles). We do not control those sites and are not responsible for their privacy practices. Please read their policies before providing them with any data.

17. 17. Data breaches

If we become aware of a security incident that materially affects your personal data, we will notify you and, where required, the relevant supervisory authority, in accordance with applicable law. We will also take steps to contain the incident, remediate the underlying cause, and reduce the risk of recurrence.

18. 18. Changes to this policy

We may update this Policy from time to time to reflect changes in our practices, our services or the law. Material changes are announced on the Platform. The effective date at the top of the document shows when the current version came into force.

19. 19. Detailed provisions & specific retention periods

Account data. Your name, email address, phone (optional) and password hash are held for the life of your Account and for up to seven (7) years after Account closure to meet financial-services and AML record-keeping requirements. On closure, we may retain the minimum data needed to defend against subsequent claims and to comply with the law.

Identity data (KYC). Full legal name, country of residence, identity document type and reference number, and any evidence of source of funds or source of wealth are held for the same statutory period as Account data. Access is restricted to authorised staff and audited.

Transaction data. Deposit records (including TXIDs and coin type), plan history, daily-return ledgers, withdrawal records, referrals and reward activity are retained for as long as they may be subject to a regulatory, tax or audit request — typically the same seven-year window.

Support data. Ticket subjects, message bodies, contact-form submissions, and internal notes attached to your Account are retained for up to five (5) years so that we can give context to future queries and to defend our position if a dispute arises. Sensitive attachments are subject to shorter, need-based retention.

Technical data. Session identifiers, IP addresses, user-agent strings and diagnostic logs are typically retained for ninety (90) days. Longer retention is only used where a specific security investigation is open, or where required by law.

Aggregated & anonymised data. Once data has been genuinely anonymised so that there is no realistic way to re-identify a specific person, it is no longer personal data and may be retained indefinitely for reporting and product-improvement purposes.

Data minimisation. We collect the minimum personal data needed for each specific purpose. Fields marked optional on our forms are optional; your Account works without them. Where we can complete a task without collecting personal data at all, we do that.

Aggregated reporting. We may combine anonymised data from many Accounts to produce reports about the health of the Platform (for example daily active users, average deposit size, popular plans). These reports do not identify you and are not personal data.

Complaints. If you are unhappy with how we handle your personal data, please contact us first so we can address the issue. If you remain dissatisfied you may have the right to complain to a data-protection supervisory authority in your country. That right does not replace any right you have to raise a court claim.

Records of processing. We maintain internal records of the personal data we process, the purposes for which we process it, the recipients we share it with, and the retention periods we apply. These records are reviewed periodically by our compliance function.

Vendor management. Where we engage service providers to process personal data on our behalf, we require them by contract to protect the data to at least the standard set out in this Policy, to use it only on our instructions, and to notify us promptly of any incident affecting it.

Escalation. For urgent privacy matters (for example a suspected compromise of your Account) mark the subject line "Urgent Privacy" so we can prioritise the request.

20. 20. Contact

Privacy questions and rights requests: contact us via the [contact page](#) or email support@universalquantum.net. Mark the subject line "Privacy" so the request reaches the right team.

© 2026 Universal Quantum. All rights reserved. This document is provided for transparency and does not constitute financial advice.