AML & KYC POLICY

---

1. INTRODUCTION

We are REVELTRY, an application provided and maintained by Wondr Technologies UK Limited (company number 16979480) ("we", "us" or "our") of C/O Gs Verde Accountants The Mezzanine, 1 The Square, Bristol, City Of Bristol, United Kingdom, BS1 6DG.

This policy aims to check identity, user safety, and transparency.

We apply KYC and AML controls to verify users, prevent fraud, and protect the platform against criminal misuse in the United Kingdom.

2. These measures support:

i. Fair play across betting and gaming products
ii. User safety and account protection
iii. Transparency in how accounts are opened and used
iv. Compliance with regulatory requirements and reporting obligations
v. ID verification and document submission requirements
vi. Every new user must complete ID verification before accessing full services, and maybe asked for information during the account lifecycle to meet regulatory requirements.

3. Documents requested may include:

i. Government-issued photo identification to confirm name, age, and nationality
ii. Proof of address dated within an acceptable time frame
iii. Evidence that the payment method is owned by the account holder
iv. Further information to support identity check, source of funds, or source of wealth where risk dictates
v. AML security measures and transaction monitoring
vi. We implement layered security measures to prevent money laundering and illegal activity, combining automated and manual controls to address suspicious activity.

4. Key controls include:

i. Real-time and retrospective transaction monitoring across deposits, withdrawals, and gameplay
ii. Automated detection rules and alerts calibrated to risk indicators
iii. Enhanced due diligence for high-risk scenarios, including source of funds and source of wealth assessment
iv. Review and escalation of large or unusual transfers, patterns, or rapid movement of funds
v. Customer and product risk scoring that informs ongoing oversight
vi. Sanctions and PEP screening against UK and international lists, including OFSI notices
vii. Reporting obligations fulfilled by submitting suspicious activity reports to the UKFIU (NCA) under the Proceeds of Crime Act 2002 and Terrorism Act 2000, where required by law.

5. Prohibited activities supporting account protection

i. To uphold KYC and AML standards, certain activities are restricted and may lead to enforcement if detected.
ii. Prohibited actions include:

a. Creating multiple accounts or impersonating another person
b. Submitting forged, altered, or stolen documents during document submission
c. Attempting to launder criminal proceeds or obscure the source of funds
d. Manipulating systems, odds, software, or payment flows
e. Sharing,selling, or otherwise transferring account access
f. Using third-party or anonymous payment instruments
g. Misrepresenting identity, income, or the purpose of transactions

6. Consequences for non-compliance and suspicious activity

Breaches of this policy or failures during identity check and due diligence may result in immediate action, in line with UK law and licence conditions. Enforcement may include temporary or permanent account suspension, freezing or confiscation of funds linked to suspicious activity, cancellation of bets or winnings, reporting to competent authorities where applicable.

7. User responsibilities for accurate personal data.

Users must provide accurate, complete, and up-to-date personal data during registration and throughout the customer relationship. Verification requests must be completed promptly and any additional document submission must be supplied within stated time frames. Only payment methods owned and controlled by the account holder may be used.

Users should report suspicious activity or security concerns to customer support without delay. Actions should align with responsible gaming guidance and legal duties.

8. Fair play, transparency, and ongoing protection

We are committed to fair play and transparency to maintain a safe, compliant environment for all users. The platform operates under these principles:

i. Compliance with KYC, AML, and CTF standards, including UKGC rules
ii. Confidentiality and protection of personal data under the UK GDPR and Data Protection Act 2018
iii. Ongoing monitoring for suspicious activity and timely escalation
iv. Prevention of manipulation, collusion, and other unfair behaviour
v. User support on safety matters, security measures, and reporting obligations
vi. Shared responsibility between the operator and users for account protection
vii. Equal conditions and consistent application of rules