KYC POLICY

1. Introduction and Policy Objectives

1.1. Company Name and Scope of Activities

The objective of this Know Your Customer (KYC) Policy (the "Policy") is to define the fundamental procedures and requirements for identifying and verifying Users, as well as to prevent money laundering and terrorist financing.

This Policy applies to all Users utilizing the Services provided by Joycee Gifts Ltd (the "Company") through its official platform: https://joycee.gifts.

1.2. Policy Objectives

This Policy extends to all Users of the Company, including both individuals and legal entities, as well as the Company's employees and other authorized parties involved in business operations related to the sale, purchase, or exchange of Digital Products.

Note (UK Context): This Policy is designed to align with UK anti-money laundering (AML) and counter-terrorist financing (CTF) regulations, including:

- The Proceeds of Crime Act 2002 (POCA)
- The Terrorism Act 2000
- The Money Laundering Regulations 2017 (MLR 2017), as amended

1.3. Scope of Application

All employees, business counterparties, and partners associated with the Company are required to comply fully and unconditionally with the provisions set forth in this Policy.

Non-compliance may result in disciplinary, administrative, or legal liability under applicable legislation and the Company's internal compliance framework.

2. Legislative and Regulatory Framework

- **KYC (Know Your Customer):** Procedures to identify, verify, and assess Users in order to prevent money laundering and fraudulent activities.
- **AML (Anti-Money Laundering):** Measures to detect, mitigate, and eliminate the risks of money laundering.
- **CTF (Counter-Terrorist Financing):** Strategies to combat the financing of terrorist activities.

- **CDD (Customer Due Diligence):** Verification process for assessing User risk and confirming identity.

- **Competent Authority:** Regulatory body responsible for AML/CTF oversight (e.g., FCA, FIUs, HMRC).

- **GDPR/UK GDPR (General Data Protection Regulation):** Frameworks governing the protection and processing of personal data in the EU and the UK.

3. Applicable Legislation

3.1. EU Directives

- Directive (EU) 2015/849 (4AMLD)

- Directive (EU) 2018/843 (5AMLD)

- Directive (EU) 2018/1673 (6AMLD)

3.2. UK AML/CTF Laws

- Proceeds of Crime Act 2002

- Terrorism Act 2000

- MLR 2017

- FCA and HMRC Guidance

3.3. Data Protection Laws

- EU GDPR (Regulation 2016/679)

- UK GDPR & Data Protection Act 2018

3.4. FATF Recommendations

- International standards for AML/CTF compliance

3.5. National Implementation

- National laws of EU Member States

- UK frameworks via FCA, HMRC, OFSI

4. Core Principles

4.1. Know Your Customer (KYC)

The Company enforces robust procedures to identify and verify Users to mitigate AML/CTF risks.

4.2. Risk-Based Approach

The Company applies verification based on the User's risk profile, including PEP status, jurisdiction, transaction behavior, and delivery channels.

4.3. Confidentiality

Personal Data collected is protected under GDPR/UK GDPR and is processed only within the legal framework.

4.4. Risk Management

Ongoing risk assessments are performed to ensure alignment with applicable AML/CTF laws.

5. Roles and Responsibilities

5.1. Board of Directors or Sole Director

- Reviews and formally approves this Policy on a periodic basis.
- Ensures adequate resources are allocated for the effective implementation and enforcement of the Policy.
- Maintains compliance with all applicable EU and UK anti-money laundering (AML) and counter-terrorist financing (CTF) regulations.

5.2. Compliance Officer

- Oversees the development, execution, and continuous monitoring of the Company’s compliance framework.
- Conducts internal audits and employee training sessions to reinforce AML/CTF compliance practices.
- Liaises with competent authorities, including financial intelligence units and regulatory bodies such as the FCA in the UK.
- Manages the reporting process for suspicious transactions, ensuring full compliance with EU and UK legal obligations for Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs).

5.3. Customer-Facing Employees

- Perform CDD checks in strict adherence to KYC procedures, which include the collection and verification of identification documents and registration data.

- Immediately escalate any detected suspicious activities or transactions to the Compliance Officer for further review.

- Ensure full adherence to UK AML laws, including POCA 2002, the Terrorism Act 2000, and the Money Laundering Regulations 2017 (MLR 2017), particularly for transactions involving UK-based clients or business counterparts.

6. KYC Procedures

6.1. Customer Identification Program (CIP)

- **Individual Users:** Full name, DOB, nationality, address, contact info, ID documents, and proof of address.

- **Corporate Entities:** Company name, registration, UBOs, signatories, and certified extracts.

6.2. Verification

- Validate the accuracy and consistency of customer-provided information and supporting documents.

- Utilize independent and trustworthy data sources, such as government databases, electronic identity verification systems, and financial records.

- For high-risk customers, conduct Enhanced Due Diligence (EDD) as per EU and UK AML compliance requirements, ensuring deeper scrutiny into their financial and transactional activities.

6.3. Ongoing Review

- Regularly update User's information based on a predefined periodic schedule (at least annually for high-risk customers) or when significant changes occur in beneficial ownership structures.

- If discrepancies or suspicious factors arise, request additional verification documents and initiate a reassessment of the User's risk profile.

7. Risk Segmentation

7.1. Risk Categories

- **Low Risk:** Users operating in well-regulated jurisdictions, conducting transparent business activities, maintaining a positive compliance record, and demonstrating consistent and predictable transaction behavior.

- **Medium Risk:** Users with certain risk factors, such as expanding into new markets or engaging in non-standard financial transactions, but without direct indicators of involvement in money laundering or terrorist financing.

- **High Risk:** Users associated with high-risk or sanctioned jurisdictions, individuals classified as Politically Exposed Persons (PEPs), entities with non-transparent ownership structures, or transactions displaying unusual or potentially fraudulent activity patterns.

7.2. Enhanced Due Diligence (EDD)

For Users identified as high-risk, the Company enforces Enhanced Due Diligence (EDD) procedures, which include:

- Requesting additional supporting documents, such as financial statements and evidence of the source of funds.

- Conducting in-depth verification of income sources and capital origins.

- Increasing the frequency of transaction monitoring to detect irregular patterns.

- Gathering references or performing background checks, including media scans, sanction list screenings, and terrorist financing watchlist reviews.

8. Transaction Monitoring

8.1. Ongoing Monitoring

- Continuously monitors for irregularities.

8.2. Red Flags

- Includes mismatched activity, false documentation, unusual frequency/volume.

8.3. Reporting

- EU: Reports to local FIUs.

- UK: Reports to NCA in line with POCA and MLR 2017.

9. Data Protection

9.1. Retention

- The Company retains User identification and verification data for a minimum of five (5) years from the termination of the business relationship or the date of the last recorded transaction, as required by Article 40 of Directive (EU) 2015/849.

- In the UK, retention periods must comply with MLR 2017 and regulatory guidance from HMRC and FCA, which typically enforce the five-year minimum but may require extended retention in certain cases.

9.2. Personal Data Protection

- The Company ensures full compliance with data protection regulations, including the General Data Protection Regulation (GDPR) (EU Regulation 2016/679) and the UK GDPR/Data Protection Act 2018, depending on jurisdiction.

- Implements robust technical and organizational security measures, such as encryption protocols, controlled access systems, and internal information security policies to safeguard sensitive customer data.

- Personal Data is processed strictly for KYC/AML/CTF purposes and is only used within the legal framework and User consent requirements, where applicable.

9.3. Confidentiality

- Access to User data is strictly limited to authorized personnel, based on their job functions.

- Unauthorized disclosure of information is strictly prohibited and will result in disciplinary action, in accordance with the Company's internal policies and relevant EU/UK legal provisions.

10. Staff Training

10.1. Training Programs

- Covers AML/CTF, GDPR, internal procedures.

10.2. Professional Development

- Required for Compliance Officers and relevant employees.

11. Policy Review and Amendments

11.1. Responsibility

- Compliance Officer & management.

11.2. Updates

- Require formal approval before enforcement.

12. Breach and Enforcement

12.1. Violations

- Include falsified info, failed due diligence, ignored STR/SAR duties.

12.2. Liability

- Disciplinary action.

- Civil/regulatory penalties.
- Criminal charges under POCA/Terrorism Act if applicable.

13. Final Provisions

13.1. Applicability

- Mandatory for all departments and personnel.

13.2. Priority of Law

- Applicable laws override this Policy in case of conflict.

14. Contact Information

- General Support: support@joycee.gifts
- Compliance: compliance@joycee.gifts
- Company: Joycee Gifts Ltd
- Address: 311 Shoreham St, Highfield, Sheffield S2 4FA, United Kingdom
- Website: https://joycee.gifts/

EU Competent Authorities

• National Financial Intelligence Units (FIUs) of respective EU Member States.

• Licensing and supervisory authorities, based on the jurisdiction and business activity of the Company.

UK Competent Authorities

• National Crime Agency (NCA) – Responsible for Suspicious Activity Report (SAR) filings.

• Financial Conduct Authority (FCA) – If the Company falls under its regulatory supervision.

• HM Revenue & Customs (HMRC) – Supervising AML/CTF compliance for specific business sectors.

• Office of Financial Sanctions Implementation (OFSI) (HM Treasury) – Ensuring compliance with UK financial sanctions.

Last updated: 23.10.2025