Privacy Policy

Pocket Money Adventures CIC | Version 1.4

Effective: 2 October 2026 | Review: 2 October 2027 or sooner on relevant change

Policy owner: Nathan Waldron, Director | Signatories: Nathan Waldron and Bernadette Houlton | Approved policy issue

Adopted by Pocket Money Adventures CIC on 2 October 2026.
Signed electronically: Nathan Waldron, Director and Designated Safeguarding Lead.
Signed electronically: Bernadette Houlton, Director and Deputy Designated Safeguarding Lead.
Typed electronic signatures in the established policy format.

Who we are

Pocket Money Adventures CIC, company 16994988, is the controller for its own operational records. Registered office: 68 Nottingham Road, Eastwood, Nottingham, NG16 3NQ. Data protection contact: dpo@pocketmoneyadventures.co.uk; general: hello@pocketmoneyadventures.co.uk; safeguarding: safeguarding@pocketmoneyadventures.co.uk; complaints: complaints@pocketmoneyadventures.co.uk. Existing records state ICO registration ZC124930; current registration and renewal must be checked in the evidence register. Nathan is the data protection lead; no statutory DPO appointment is asserted.

Routine child-data rule

Zero Child Data applies to routine learning, access and evaluation: no child names, accounts, personal finances, individual tracking or school-held match-code keys are collected by PMA. Standard PMA sessions do not involve PMA photographing or filming identifiable children. Necessary safeguarding, accident or legal records are an exception and are minimised, protected and shared lawfully. Pseudonymised codes are not automatically anonymous. Research beyond safe aggregates requires a separately approved protocol, lawful basis, privacy information and ethics arrangements before collection.

Adult and operational data

Depending on your interaction, we process adult contact and organisation details, correspondence, booking logistics, contract and payment records, preferences and consents, voluntary feedback, recruitment and worker records, access requirements and necessary safeguarding records. Do not send bank passwords, PINs, child records or household financial documents. In any supported adult service, participants keep their own financial figures.

Purposes and lawful bases

We identify an Article 6 basis for each actual purpose: consent for opted-in marketing and optional follow-up; contract where necessary for a contract with the individual; legitimate interests for proportionate administration and organisation-contact logistics following assessment; legal obligation only where the specific duty applies; vital interests where applicable. A school or company contract does not automatically make Article 6(1)(b) appropriate for every employee's contact data. Safeguarding does not require consent where another lawful basis applies. Special-category and criminal-offence data need the additional applicable conditions and safeguards, not consent by default.

Evaluation and research

Standard reporting uses safe aggregates and suppresses small cells or identifying quotations. School-held match keys never come to PMA. Codes can remain personal data if re-identification is reasonably possible. Separate research requires approved purpose, minimisation, roles, ethics, privacy information and any required DPIA before collection. Optional participation or research refusal does not remove access to the educational session.

Sharing and processors

Information is shared only as necessary with hosts, authorised workers, contracted technology suppliers, accountants, banks, insurers, regulators or safeguarding authorities. Sponsors receive safe aggregate reporting, not participant identities. Maintain an actual supplier/processor register and appropriate contracts. No unsupported promise is made that Microsoft, Mailchimp or another supplier processes only in the UK, or that international-transfer terms have already been confirmed. Assess location, subprocessors and appropriate transfer safeguards before use. We do not sell personal data.

Retention

Keep operational contact and optional supported-service records for the necessary purpose, normally no more than 12 months after last contact unless another documented schedule applies. Mailing lists: until withdrawal or two years' inactivity, reviewed regularly. Financial/contract records: normally six years, longer where law or grant terms require; grant evidence normally at least seven years where required by the grant controls. HR and recruitment records require category-specific justification; do not keep every unsuccessful application for six years by default. Research retention is set in its approved protocol; truly anonymous findings may be retained longer. Safeguarding, allegation and incident records follow documented applicable requirements, legal holds and specialist advice; KCSIE does not impose one universal age-25 rule on all PMA records.

Your rights and requests

You can request access, correction, erasure, restriction, portability where applicable, object or withdraw consent. Rights depend on the lawful basis and applicable exceptions. Make requests in any format to any PMA contact; dpo@ is the preferred route, not a condition. Respond without undue delay, normally within one calendar month. Necessary identity/authority information or reasonably required SAR clarification can affect the clock under current rules; log and explain it. Complexity or multiple requests can justify up to two additional months with timely reasons, not a general delay allowance. A child's right belongs to the child; parental authority, competence and best interests are assessed, without a blanket under-13 rule.

Marketing and websites

Optional marketing and parent prompts require the appropriate permission and a clear opt-out. Service messages may still be necessary. Website logs and device information can be personal data. Use the current Cookie Policy and an actual per-site technology inventory; do not assume IP truncation or anonymity. Child-facing access to the free story does not require registration or an email address.

Security, breaches and complaints

Use least privilege, secure storage, MFA where available, safe sharing and tested deletion. Verify the controls on the actual systems. Log every personal-data breach. Notify the ICO within 72 hours of awareness where the Article 33 threshold applies; notify affected people without undue delay where the Article 34 high-risk threshold applies, subject to its exceptions. You may complain directly to the ICO at ico.org.uk or 0303 123 1113; you need not exhaust PMA's complaints procedure first.

Issue control: current approved issue dated 2 October 2026. Earlier issues are archived. Policy approval does not complete host agreements, individual acknowledgements or venue checks.