

Record of Processing Activities

Pocket Money Adventures CIC | Version 1.1

Effective: 2 October 2026 | Review: 2 January 2027 and every material change 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.

Controller and status

Pocket Money Adventures CIC is controller for its own administration, HR, finance and safeguarding records. Nathan is data protection lead. This issue replaces the old assertions of UK-only processing, universal processor status, anonymous match codes and all controls already implemented. Verify the actual supplier register, contracts, security and transfers before new processing.

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.

Bookings and partner contacts

Subjects: adult school/host/sponsor contacts. Data: identity, role, business contact, logistics, agreement and correspondence. Purpose: arrange and deliver services and funding. Basis: assessed legitimate interests, or contract with an individual where applicable. Recipients: authorised workers, host and actual contracted systems. Retention: necessary relationship period; contractual/finance records normally six years. Safeguards: minimum access, secure sharing, MFA where available and verified.

Optional adult support, follow-up and marketing

Subjects: consenting adults. Data: necessary contact, functional access needs, choices and minimal service notes. Basis: purpose-specific consent for optional follow-up/marketing and agreed basis for arranging service. Additional sensitive-data condition where needed. Optional service contacts normally 12 months after last contact; lists until withdrawal or two years' inactivity. No child records or personal financial documents. Suppliers must be recorded by actual name and contract before use.

Evaluation and research

Standard delivery: safe aggregate feedback only. Separate approved research: document actual subjects, fields, code status, roles, basis, consent/ethics, recipients, retention and DPIA before use. Never claim pseudonymous data is automatically anonymous. Source pilot dates and comparator promises are historical; they are not a new live protocol.

HR, volunteers and vetting

Subjects: applicants, workers and volunteers. Data: role/history, references, identity/right to work as required, payroll and minimal vetting record. Bases: applicable contract, employment/legal obligation and assessed legitimate interests; additional conditions for sensitive/criminal data. Recipients: authorised decision-makers and actually engaged payroll, HMRC, pension and DBS bodies. Unsuccessful applicants normally six months; worker records category-specific, normally up to six years after exit where justified. DBS copies normally no longer than six months unless justified.

Safeguarding and incident records

Subjects: anyone whose protection/incident record is necessary, including children. Data: minimal facts, exact words, actions and recipients. Select a justified Article 6 basis and additional Article 9/10/DPA conditions as applicable. Recipients: relevant host lead, local authority, LADO, police, insurer or other lawful recipient. Retention: category-specific, applicable requirements and holds, reviewed; no universal age-25 rule. Access: restricted safeguarding/incident file with independent escalation.

Finance and compliance

Subjects: payers, suppliers, directors, workers and contacts. Data: invoices, agreements, bank/payment references, approvals, conflicts and reporting. Bases: contract where appropriate, legal duties and legitimate interests. Recipients: bank, actual payment/accounting providers, HMRC, auditors and funders as necessary. Retention normally six years; grant records normally at least seven where required. No child identities in funder reporting.

Websites, complaints and rights

Website device/log data: document actual hosting, security, cookie/analytics purposes, consent or exception, supplier, retention and transfers. Complaints and rights records: minimum necessary facts, correspondence, actions and outcomes; basis appropriate to complaint/rights handling; restricted access; normally six years where justified. Every actual system and processing change must be added to the live operational register.

Implementation checklist

For each actual activity record: controller/processor role; owner; system and supplier; purpose; subject/field list; lawful basis and sensitive-data conditions; recipients; transfers and safeguard; retention/deletion date; security evidence; DPIA/contract reference; last verification. No new processing is authorised by an incomplete row.

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.