

Information Sharing and Supported Connection Protocol

Pocket Money Adventures CIC | Version 1.1

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.

Current operating requirements

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.

Separate optional adult supported connections from necessary safeguarding sharing. Agree safe contact channels and the exact minimum information for an optional referral; do not send without the recorded choice. Safeguarding or other lawful required disclosure may use a different basis. Record the Article 6 basis and additional sensitive-data condition where relevant.

Detailed policy and procedures

Information Sharing and Supported

Connection Protocol

This protocol sets out how Pocket Money Adventures CIC handles information about the families who take part in our community sessions, and how we help a household reach another service when they want support we do not provide. Why this document exists Pocket Money Adventures delivers financial education and non-regulated money guidance. We are not an advice service, and we do not run a referral scheme. Sometimes a parent or carer tells us about a need that belongs with someone else, and they want help making contact. This protocol makes that safe: the adult decides, the adult is present, and the least possible information travels with their explicit consent. It also serves as our information sharing arrangement where a funder or partner requires one, and it applies whether or not any other organisation has signed an agreement with us.

1. Scope and roles

This protocol applies to all participant information collected in community delivery. Pocket Money Adventures CIC is the data controller for the information we collect and hold. Where a household contacts another service, that service is a separate controller for whatever the household tells it directly. The organisation is registered with the Information Commissioner's Office, registration ZC124930. This protocol operates alongside our Privacy Policy and our Children and Adult Safeguarding Policy.

2. What we collect, and what we do not

At intake we collect only what the service needs:

- the adult's name and preferred contact details;
- confirmation of residence in the delivery area, and the first part of the postcode;
- the age band of participating children, not their names where this can be avoided;
- accessibility and communication requirements;
- broad categories of the pressures the household would like help with;
- a financial position the adult places themselves in, using a simple scale, where they choose to; and
- consents, recorded separately for follow-up contact, for any supported connection, and for use of an anonymised case study. We do not collect bank statements, account numbers, credit files, detailed debt schedules or benefit award records. We do not ask children for any information about their household's money, and no child's view of family hardship is ever recorded. Adults keep their own figures: where a household uses a budgeting or entitlement tool with us, the numbers stay with them and we record only that the tool was used.

3. Lawful basis

We process participant information on the basis of consent for contact and follow-up, and on the basis of legitimate interests for the anonymised monitoring we report to funders. Consent is asked for separately for each purpose, is recorded, and can be withdrawn at any time without affecting a household's ability to take part. Where information indicates a risk to a child or an adult at risk, we may share without consent, as set out in section 6.

4. Supported connections

Where an adult wants help reaching another service, one of three routes is used, and the adult chooses:

- Assisted contact. We help the adult make contact themselves while they are with us, by telephone, web chat or a public form. Nothing about the household travels without them. This is our normal route;
- Consented minimum-data contact. Where a service operates its own referral route and the adult prefers it, we send only the minimum information that route requires, with the adult's explicit and recorded consent, and the service contacts them directly. We do not ask for case information back; and
- Declining. An adult may take the information away and act later, or not at all. This is recorded as offered and declined, and changes nothing about their participation. In every route we record only: that a connection was offered; the type of service; whether consent was given; whether contact was initiated; and whether the household reports that first contact happened. We do not record what the other service then did.

5. What we never do

- We do not provide regulated financial advice, debt solutions, benefit determinations or product recommendations, and we do not hold ourselves out as able to;

- we do not pass household information to any organisation without the adult's explicit, recorded consent, except as required by section 6;
- we do not sell, rent or use participant information for marketing;
- we do not use a director's personal professional qualifications as though they were held by the organisation; and
- we do not create records simply because a monitoring form has a field for them.

6. Safeguarding overrides consent

Where information suggests a child or an adult at risk is at risk of harm, we share what is necessary with the appropriate authority without requiring consent, in line with our Children and Adult Safeguarding Policy and Staffordshire's safeguarding partnership procedures. Wherever it is safe to do so, we tell the person what we are sharing and why. Financial abuse, coercive control and domestic abuse are treated as safeguarding matters, not as money problems.

7. Storage, access and retention

- Records are held in access-controlled systems, available only to those who need them for delivery, safeguarding or reporting;
- identifiable participant records are retained for twelve months after a household's last contact, then deleted, unless a safeguarding record requires longer under our safeguarding policy;
- anonymised monitoring information may be retained for the life of the funded project and any audit period that follows;
- consent records are retained for as long as the information they relate to; and
- case studies are published only with separate written consent, and only in a form that cannot identify the household or any child.

8. Reporting to funders

Where a funder requires monitoring returns, we provide anonymised, household-level information: a reference that is not the household's name, broad geography, household composition bands, engagement and outcome fields, and the household's own self-placed financial position where they have given it. Case studies are anonymised and separately consented. Participants are told at intake that anonymised information is reported in this way.

9. Participant rights

Every participant receives a plain-language privacy notice at intake. Anyone may ask what we hold, ask for it to be corrected or deleted, withdraw consent, or complain, by contacting hello@pocketmoneyadventures.co.uk. Requests are answered within one month. Anyone dissatisfied may complain to the Information Commissioner's Office.

10. Responsibility, breaches and review

The Director acting as data protection lead is responsible for this protocol. Any suspected breach is reported to them the same day, assessed, recorded, and reported to the Information Commissioner's Office within seventy-two hours where the threshold is met, with affected people told where the risk to them is high. Everyone delivering sessions is briefed on this protocol before their first session. It is reviewed annually, or sooner if our delivery, funding or reporting arrangements change.

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.