

DPIA Pause Plan Prepare

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

Processing gate and assessment status

This is a project planning DPIA. The supplied source is a proposed Tamworth October 2026-March 2027 service, not proof of an awarded contract. Confirm commissioner, geography, dates, field list, reporting platform, suppliers, lawful bases, consent routes and safeguards before any intake. No processing starts until controls and residual-risk acceptance are evidenced. If unmitigated high risk remains, seek ICO prior consultation where required.

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.

Detailed policy and procedures

Data Protection Impact Assessment

This assessment covers Pause, Plan, Prepare, the family financial resilience service delivered by Pocket Money Adventures CIC in Tamworth from October 2026 to March 2027. It is maintained as planning evidence because the service processes information about households in financial difficulty, including families with young children, and reports monitoring information to a funder. Conclusion, stated first The actual residual risk has not yet been verified. The service is designed around collecting very little, keeping figures with the participant, and requiring consent for every onward contact. Verify and record the controls in section 5 before delivery begins.

1. The processing

We collect intake information from adults who choose to attend, record which activities and tools they used and what action they chose, and follow up at about four weeks and again later where they agreed. The source proposal envisages anonymised quarterly monitoring to Staffordshire County Council through Plinth, subject to the actual contract and verified platform arrangements, including household counts, broad geography, engagement, chosen actions, outcome categories and self-placed financial position, plus at least two separately consented anonymised case studies.

2. Necessity and proportionality

Each field is collected for a stated purpose set out in the Participant Privacy and Consent document. Fields the funder does not require and delivery does not need are not collected. Children's names are avoided; only an age band is recorded. No financial documents are collected. Participants keep their own figures, which removes the largest category of sensitive data the service could otherwise hold.

3. Lawful basis

Processing Basis

Arranging attendance Consent, given at booking or intake

Follow-up contact Consent, recorded separately and withdrawable

Sending information to another service Explicit consent, given each time

Anonymised funder reporting Legitimate interests, balanced against participant rights; no identifying data leaves the organisation

Safeguarding disclosure Legal obligation and vital interests; substantial public interest condition for any special category data

Case studies Explicit, separate consent

4. Risks identified

- information about financial difficulty is sensitive in context and could cause distress or stigma if disclosed;
- a household may include a person at risk of domestic or financial abuse, so contact through the wrong channel could cause harm;
- children are present in sessions, though not the subject of the record;
- special category or criminal-offence data could arrive unsolicited through a disclosure;
- a supported connection could result in more information travelling than the participant expected;
- a case study could identify a household in a small community; and
- records could be retained longer than needed, or accessed by people who do not need them.

5. Controls

- Minimisation. A fixed field list; nothing collected because a form has a box for it. No financial documents. Age bands, not children's names.
- Separation. Private money conversations never happen while a child is being supervised, and never in front of other participants.
- Consent design. Separate, recorded, withdrawable consents for follow-up, connection, information sending and case study; refusal changes nothing about participation.

- Safe contact. Contact channel agreed with the participant, and never a channel that may be seen by a person they have identified as a risk.
- Connection rule. Participant-led contact is the default; where information is sent, the participant is told exactly what will be sent before it goes, and only the minimum the route requires.
- Case studies. Anonymised, separately consented, and checked so that no combination of details identifies a household.
- Access. Role-based access; only those delivering, supervising or reporting can see records.
- Retention. Identifiable records twelve months after last contact; anonymised monitoring for the project and audit period; safeguarding records per statutory requirement.
- Unsolicited sensitive information. Recorded only where necessary for safeguarding, handled under the Adult Safeguarding and Trauma-Informed Response procedure.
- Training. Everyone briefed on this assessment and the consent process before their first session.
- Breach route. Reported to the data protection lead the same day, assessed, and notified to the Information Commissioner's Office within seventy-two hours where the threshold is met.

6. Residual risk and sign-off

Assess actual residual risk after the controls are verified. Prior consultation is required where high risk remains that cannot be mitigated. This assessment is reviewed if the service changes, if a new data field is requested by the funder, or annually, whichever comes first. Planning issue approved by Nathan Waldron as data protection lead; operational processing authorisation and residual-risk acceptance remain separate.

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.