

# Confidentiality and Information Sharing Procedure

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.

Consent is not a prerequisite for necessary lawful child-safeguarding sharing. Record necessity, proportionality, lawful basis, any special-category/criminal-data condition, recipient and action. Preserve confidentiality, restrict access and follow the current retention schedule. Do not delay urgent protection or promise absolute secrecy.

## Detailed policy and procedures

### Confidentiality and Information Sharing Procedure

This procedure supports the Pocket Money Adventures CIC Safeguarding Policy. It explains how we record safeguarding concerns and how we share information safely and lawfully when needed.

#### 1. Purpose

To ensure safeguarding concerns are recorded accurately and shared appropriately so children and adults at risk are protected.

#### 2. Scope

Applies to all directors, employees, contractors and volunteers delivering or supporting PMA activities, particularly in schools and community settings.

#### 3. Principles

- Need-to-know: information is shared only with people who need it to keep someone safe.

- Proportionate: we share the minimum necessary information.
- Timely: safeguarding information is recorded and escalated without delay.
- Accurate: we record facts, using the person's own words where relevant.
- Secure: records and communications are stored and transmitted securely.

#### 4. What must be recorded

A written record must be made as soon as possible (normally within 24 hours) for:

- a disclosure or allegation made by a child or adult at risk
- a concern observed by staff/volunteers (e.g., behaviour, injury, worrying statements)
- an incident during delivery that has safeguarding implications
- an allegation against a person in a position of trust (staff/volunteer/director).

Records should include:

- date, time and location
- names of people involved (where known) and role/relationship
- what was seen/heard (facts) and the exact words used where relevant
- actions taken immediately
- who was informed (e.g., school DSL, local authority) and when
- the decision and rationale (why information was shared or not shared).

#### 5. Where records are kept

PMA keeps safeguarding records securely with restricted access. As PMA primarily delivers through schools, the host school/setting is usually the primary safeguarding lead and record holder.

PMA will:

- share concerns promptly with the host school/setting Designated Safeguarding Lead (DSL) and follow their reporting route
- retain only what is necessary for accountability and follow-up
- store any retained records in a restricted-access safeguarding folder (separate from general project files).

#### 6. Sharing information

We may share information without consent where it is necessary to protect a child or adult at risk, prevent serious harm, or where required by law.

In school delivery, our default route is:

- Report immediately to the host school/setting DSL (or deputy).
- If a child is in immediate danger, call emergency services (999) and then inform the school DSL.
- If the concern relates to a member of PMA staff/volunteer, escalate to PMA DSL and follow the allegations management process.

When sharing information, we record what was shared, with whom, when, and why.

## 7. Secure communication

Safeguarding information should be shared using secure methods wherever possible (e.g., the school's safeguarding reporting system, secure email, or a documented phone call).

Do not:

- share safeguarding information on social media or informal messaging apps
- store safeguarding information on personal devices
- take photos/videos of children unless authorised by the school and permitted by consent arrangements.

## 8. Retention and disposal

PMA retains safeguarding records only as long as necessary. Where the school/setting holds the primary record, PMA's retained copy (if any) will normally be limited and time-bound. Default retention approach (unless otherwise required by law or the school/setting):

- incident/concern records: minimum 7 years from the date of the record
- records relating to a child: where PMA is the record holder, retain until the child's 25th birthday where practicable, or 7 years (whichever is longer)
- after retention, records are securely deleted/shredded and disposal is logged.

## 9. Access, corrections and requests

Access to safeguarding records is limited to the PMA Designated Safeguarding Lead and authorised directors. If a data subject makes a request (e.g., subject access request), this will be handled in line with PMA's data protection process, recognising that safeguarding exemptions may apply.

## 10. Review and training

This procedure is reviewed annually. All staff/volunteers involved in delivery must receive safeguarding induction and understand how to record and escalate concerns.

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.