



Subject Access Request (SAR) Procedure

Pocket Money Adventures CIC

Version 1.0

Effective date: 24 April 2026

Review date: 24 April 2027 (or on ICO guidance change)

Approved by: Nathan Waldron, Director, acting as de facto Data Protection Officer

Pocket Money Adventures CIC

Registered office: 68 Nottingham Road, Eastwood, Nottingham, NG16 3NQ

Company No. 16994988 • ICO Registration No. ZC124930

General contact: hello@pocketmoneyadventures.co.uk

Safeguarding contact: support@pocketmoneyadventures.co.uk

Designated Safeguarding Lead: Nathan Waldron

Deputy DSL: Bernadette Houlton

Purpose:

UKGDPR Article 15 gives every individual the right to ask PMA whether it holds personal data about them, to receive a copy, and to be told about the processing. This procedure is how PMA meets that right without error or delay.

Scope:

Applies to any request for personal data held by PMA, whether from a parent about themselves, a parent on behalf of a child under 13, a pupil over 13 capable of making their own request, a staff member, a contractor, a sponsor contact, or any other data subject.

Parental requests on behalf of a child are valid under Article 8 for children under 13. Children aged 13 or over can make their own SAR and are normally the appropriate requester.

Intake:

1. A SAR can be made in any format — email, letter, phone call, in person. No form is required. PMA must not insist on a specific channel.
2. The live intake inbox is dpo@pocketmoneyadventures.co.uk (confirmed active 24 April 2026). Any other inbox that receives a SAR forwards it the same day.
3. Acknowledge receipt within 3 working days.
4. If the request is ambiguous, reach back once to clarify the scope within 5 working days. The statutory clock pauses only on ID verification, not on scope clarification.

Identity verification:

ICO guidance: verify identity proportionate to the risk. For a parent who is already on file with PMA, an email reply from the address PMA holds is usually enough. For a third-party requester, or where the information is sensitive, ask for one piece of photo ID and one proof of address, redacted to name and address only.

The one-month clock starts the day after identity is verified.

Searching for data:

PMA stores personal data in the locations documented in the Record of Processing Activities. For a given SAR, check every location relevant to the requester:

- PMA M365 tenant — mailboxes (Nathan, Bernadette, shared inboxes including complaints@ and whistleblowing@), OneDrive, SharePoint, Teams
- Mailchimp (if the subject has ever been on the mailing list)
- CRM (if adopted)
- Any paper file in the Legal + Compliance cabinet (consent slips, safeguarding notes)
- Google Analytics (IP is truncated; typically no identifiable personal data)
- Website backend (contact form submissions)

Log every search in the SAR Register (date, location, result).

Preparing the response:

5. Compile a copy of the personal data held.
6. Remove third-party personal data by redaction or exclusion — especially children's names, other parents' details, staff data, or safeguarding information about another person.
7. Apply any applicable exemptions (DPA 2018 Schedule 2–4). Common ones: confidential references, management information, negotiations, legal privilege, crime and taxation. Document the exemption used and the reason.
8. Assemble a response letter covering: what is being provided; what is not being provided and why; the data processing information required by Article 15(1)(a)–(h); the right to complain to the ICO.

Delivery:

- Free of charge. A reasonable fee only applies where the request is manifestly unfounded or excessive.
- Sent in the format the requester asked for where practicable. Default: PDF via encrypted email or via a secure link that expires in 7 days.
- Keep a copy of the sent response on file for 6 years.

Difficult cases:

- A parent requests data about their child, but the child is over 13 and has objected — refer to the child.
- A separated parent requests data about their child — confirm parental responsibility; do not take sides in a custody dispute; disclose only data about the requesting parent and the child, not about the other parent.
- The request is one of many from the same requester and appears intended to overwhelm — apply the manifestly excessive test, document, and respond with either a reasonable fee or refusal with reasons.
- A safeguarding concern is caught in the request — apply the DPA 2018 Schedule 3 Part 4 exemption where disclosure would cause serious harm. Consult the DSL before responding.

Record-keeping:

Every SAR is logged in the SAR Register (stored in the Legal + Compliance area):

- Date received, acknowledged, ID verified, searches started, response sent, closed
- Requester category (parent, pupil, staff, other)
- Scope agreed
- Locations searched

- Exemptions applied
- Outcome (provided in full / partial / refused)
- Any follow-up (ICO complaint, second request)

Breach and escalation:

If PMA fails to respond within the statutory period, the requester has the right to complain to the ICO. A breach of Article 15 can attract regulatory action. If PMA is likely to miss the deadline, invoke the two-month extension in writing, with reasons, before the one-month deadline passes.

If the SAR reveals a previously-undetected personal data breach during the search, apply the Data Breach Response Plan (72-hour ICO reporting clock) in parallel.

Linked policies and references:

- Data Protection and Privacy Policy v1.3
- Record of Processing Activities v1.0
- Privacy Policy v1.2 (public)
- Children and Adult Safeguarding Policy v1.2
- Operational Reference Hub — SAR procedure (OPREF row); ICO Right of Access guidance

Version history:

- v1.0 — 24 April 2026. Initial procedure. Aligned to ICO Right of Access guidance, DPA 2018 exemptions, and PMA's processing landscape. Intake dpo@pocketmoneyadventures.co.uk live from 24 April 2026. Review annually or on ICO guidance change.

Approved by Nathan Waldron, Director, on 24 April 2026.