Data Breach Response Plan

Pocket Money Adventures CIC

Version 1.0
Effective date: 24 April 2026
Review date: 24 April 2027
Approved by: Nathan Waldron, Director, on behalf of the Board of Directors (Pocket Money Adventures CIC)

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
Data Protection contact: dpo@pocketmoneyadventures.co.uk
Designated Safeguarding Lead: Nathan Waldron
Deputy DSL: Bernadette Houlton

Purpose

UK GDPR Article 33 requires a personal data controller to notify the Information Commissioner's Office (ICO) of a personal data breach within 72 hours of awareness, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Article 34 requires notification to affected individuals where the risk to their rights and freedoms is high. This plan is how PMA meets those obligations without hesitation.

Scope

Every personal data breach, whether accidental or deliberate, involving personal data controlled or processed by PMA. This includes: lost or stolen laptops or paper records, misdirected email containing personal data, unauthorised access to the PMA tenant, accidental publication on the website, compromised Mailchimp list, a third-party processor incident, a lost mobile phone with PMA mailbox access, a shared link sent to the wrong person.

Definitions

- Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Awareness: PMA becomes aware of the breach the moment any director, employee, contractor, or volunteer has a reasonable degree of certainty that a breach has occurred.
- Reportable: where the breach is likely to result in a risk to the rights and freedoms of a data subject (assessed against severity, volume, sensitivity, and the nature of the data).

Response steps

Step	What happens	Who	Within

1	Detection — any PMA person who suspects a personal data breach stops, secures, reports.	Any staff / contractor	Same hour
2	Notify the Director (Nathan) and Data Protection lead (Nathan, dpo@) — by email AND phone.	The reporter	1 hour of detection
3	Contain — stop the leak. Revoke shared links, change passwords, recover device, isolate mailbox, remove misdirected email. Record every action.	Director + reporter	4 hours
4	Log the breach in the Breach Register (who, what, when, scope, risk).	Director (dpo@)	8 hours
5	Risk assessment — is this likely to result in a risk to rights and freedoms of data subjects? If yes, the ICO must be notified.	Director (dpo@)	24 hours
6	ICO notification (if reportable) — via ICO Breach Reporting service. Get a reference. Record it.	Director (dpo@)	72 hours of awareness
7	Data subject notification — where the breach is likely to result in a high risk, notify affected individuals in clear and plain language without undue delay.	Director (dpo@)	As soon as reasonably possible
8	Safeguarding check — if the breach involves children's data, consult the DSL and consider LADO notification.	DSL (Nathan) + Deputy DSL (Bernadette)	Same day
9	Post-incident review — root cause, lessons, controls updated. Close out the breach register entry.	Director + Deputy DSL	10 working days
10	Board notification — material breaches are reported to the full Board at the next scheduled meeting; serious or reportable breaches are reported same day.	Director	Same day (if reportable)

Severity classification

- Low: limited data, small number of subjects, low sensitivity (for example: a marketing email wrongly addressed to one person). Not usually reportable. Still logged.

- Medium: identifiable personal data of more than a handful of subjects, moderate sensitivity, reputational risk. Likely reportable.
- High: special category data, children's data, large volume, financial data, or safeguarding information. Always reportable. Subject notification required.

Containment actions (do these in parallel with the clock)

- Revoke any shared links and expired-link access
- Force password reset on compromised accounts
- Remove any incorrect email via recall (then verify — do not assume recall worked)
- Disable compromised devices via Microsoft Intune / device management
- Back up relevant forensic evidence before deleting anything

Notification content (ICO and subjects)

When notifying the ICO, include:

- Nature of the breach — what happened
- Categories and approximate number of data subjects
- Categories and approximate number of personal data records
- Name and contact details of the data protection contact (dpo@pocketmoneyadventures.co.uk)
- Likely consequences of the breach
- Measures taken or proposed to address the breach and mitigate its effects

When notifying affected individuals, use clear and plain language, describe what happened, what PMA is doing, what the individual can do to protect themselves, and how to contact us.

Documentation

Every breach (reportable or not) is logged in the Breach Register. The register is the controlled record. The ICO can ask for it on inspection and PMA must produce it.

Record fields:

- Date of detection, date of reporting, date of containment, date of closure
- Nature and cause of the breach
- Categories of data and data subjects affected
- Whether reported to the ICO (with case reference)
- Whether data subjects were notified
- Actions taken and outcome
- Lessons learned and control changes made

Training and testing

This plan is reviewed annually. A tabletop breach exercise is run annually — a simulated breach scenario walked through by the Director, Deputy DSL, and any other data-handling personnel. The exercise outcome is recorded and controls are updated if the exercise exposes a gap.

Linked policies and references

- Privacy Policy v1.3
- Record of Processing Activities v1.0
- SAR Procedure v1.0 (PMA-SAR-001)
- Safeguarding Policy v1.3 (for breaches involving children's data)

- ICO breach reporting portal (in the Operational Reference Hub)
- ICO Personal Data Breaches Code: ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-data-breaches/

Version history

- v1.0 — 24 April 2026. Initial plan, aligned to UK GDPR Articles 33 and 34 and the ICO Personal Data Breaches Code. Review annually or on ICO guidance change.

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