

Data Breach Response Plan

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

Risk-based notification

Log every breach. Article 33: notify the ICO within 72 hours of awareness unless unlikely to result in a risk to rights and freedoms; notify late with reasons where needed and provide phased information when necessary. Article 34: notify individuals without undue delay where high risk is likely, subject to its exceptions. Severity labels guide assessment but do not automatically establish reportability. Processor incidents are notified to the controller without undue delay under the actual agreement.

Detailed policy and procedures

Data Breach Response Plan

Registered office: 68 Nottingham Road, Eastwood, Nottingham, NG16 3NQ Company No. 16994988 • ICO Registration No. ZC124930 General contact: hello@pocketmoneyadventures.co.uk Safeguarding contact: safeguarding@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 Any staff / contractor Same hour

person who suspects a personal data breach stops, secures, reports.

2 Notify the Director (Nathan) The reporter 1 hour of detection

and Data Protection lead (Nathan, dpo@) - by email AND phone.

3 Contain - stop the leak. Director + reporter 4 hours

Revoke shared links, change passwords, recover device, isolate mailbox, remove misdirected email. Record every action.

4 Log the breach in the Director (dpo@) 8 hours

Breach Register (who, what, when, scope, risk).

5 Risk assessment - is this Director (dpo@) 24 hours

likely to result in a risk to rights and freedoms of data subjects? If yes, the ICO must be notified.

6 ICO notification (if Director (dpo@) 72 hours of awareness

reportable) - via ICO Breach Reporting service. Get a reference. Record it.

7 Data subject notification - Director (dpo@) As soon as reasonably

where the breach is likely possible to result in a high risk, notify affected individuals in clear and plain language without undue delay.

8 Safeguarding check - if DSL (Nathan) + Deputy Same day

the breach involves DSL (Bernadette) children's data, consult the DSL and consider LADO notification.

9 Post-incident review - root Director + Deputy DSL 10 working days

cause, lessons, controls updated. Close out the breach register entry.

10 Board notification - Director Same day (if reportable)

material breaches are reported to the full Board at the next scheduled meeting; serious or reportable breaches are reported same day.

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. Urgent risk assessment required; apply Article 33 and Article 34 thresholds rather than an automatic label.

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 using the actual available device-management controls; do not assume Intune is deployed
- 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 v1.4
- Record of Processing Activities v1.1
- SAR Procedure v1.1 (PMA-SAR-001)
- Safeguarding Policy v1.7 (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/

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.