PrePark Data Breach Response Procedure

INTERNAL - Version 1.0 | Last updated 14 September 2026

Internal procedure for suspected personal-data breaches, including accidental disclosure, unauthorised access, loss, alteration, ransomware, credential compromise or improper destruction.

1. Immediate actions

1	Contain the incident without destroying evidence: revoke access, reset credentials, isolate affected systems or suspend integrations where appropriate.
2	Notify the internal incident lead immediately. Staff and contractors must not wait for certainty before escalating a suspected breach.
3	Preserve logs, screenshots, timestamps and relevant communications.
4	Identify what personal data, people, systems and third parties may be affected.
5	Contact relevant processors (for example Base44 or Stripe) where their systems are involved and preserve their incident references.

2. Initial assessment

Record when PrePark became aware of the breach. Assess the type and sensitivity of data, number of people affected, ease of identification, likely consequences, whether data was encrypted/protected and whether the breach is ongoing.

3. ICO notification decision

If the breach is likely to result in a risk to individuals' rights and freedoms, notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. If the assessment is incomplete, report available information and update later rather than missing the deadline.

Record the reasons for notifying or not notifying. All personal-data breaches must be documented even where notification is not required.

4. Notification to affected individuals

If the breach is likely to result in a high risk to individuals, inform affected people without undue delay unless a lawful exception applies. Communications should explain the nature of the breach, likely consequences, protective steps and a contact point.

5. Minimum breach log

Field	Record
Incident ID / owner	Unique reference and accountable lead.
Awareness time	Date/time PrePark became aware.
Description	What happened and how detected.
Data / people	Categories and approximate numbers affected.
Risk assessment	Potential harm and likelihood.
Containment	Actions taken / outstanding.
ICO decision	Report/not report, time and rationale.
Individual notification	Who was notified, when and how.
Supplier actions	Processor/vendor contacts and responses.
Lessons learned	Root cause, remediation and control changes.

6. Post-incident review

After containment, conduct a root-cause review, correct control weaknesses, update risk assessments, consider credential rotation or code changes, and document lessons learned. Serious incidents should be reviewed by senior management.

7. Contacts

Internal breach lead: [INSERT ROLE/NAME] Privacy contact: info@prepark.co.uk ICO reporting route: use the current ICO personal-data breach reporting service.