DATA BREACH & SECURITY INCIDENT PROCEDURE (2026)

Adopted: [11/03/26] Next review: March 2027 Owner: Parish Manager

1. PURPOSE

To ensure all personal data breaches are identified, contained, assessed, logged, reported and learned from in line with UK GDPR.

2. DEFINITION

A personal data breach is any security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. FIRST 24 HOURS – ACTIONS

1) Contain: stop further loss; revoke access; recall emails.
2) Report: immediately inform the Parish Manager via manager@oakthorpedonisthorpeandacresford-pc.gov.uk.
3) Log: open a Breach Log entry (time, systems, data types, people affected).
4) Preserve: keep evidence (emails, logs, device state).
5) Assess risk: harm to individuals (financial, identity, distress).
6) Decide ICO reporting: within 72 hours if risk is likely.
7) Remediate: reset passwords, patch, inform processors.

4. ICO NOTIFICATION (≤72 HOURS)

Notify if risk to rights/freedoms is likely. Record decision and rationale in the Breach Log. The report includes nature of breach, categories/volume, likely consequences, measures taken.

5. INFORMING INDIVIDUALS

Notify without undue delay if high risk. Use plain language, include what happened, what data, likely consequences, actions taken, advice, and contact point.

6. BREACH LOG (MINIMUM FIELDS)

Reference; dates/times; reporter; description; systems; categories/volume of data; risk rating; ICO decision; notifications sent; remediation; lessons learned; closure sign-off.

7. POST-INCIDENT REVIEW (≤14 DAYS)

Identify root cause; update controls; provide targeted training; update policies; verify closure.

8. RESPONSIBILITIES

Parish Manager leads; Chair provides oversight for serious incidents; all users must report immediately; processors must notify us without undue delay.

ersion number	Purpose/change	Author	Date
0.1	Initial draft	KG	7/20
0.2	Amended	KG	7/22
0.3	Amended	KG	05/03/26