

Bishops Lydeard and Cothelstone Parish Council

Security Incident Response Policy

Adopted by the Council on 14th November 2018.

Reviewed: 13th May 2026

Due for next Review: May 2027

This Council understands that planning for a breach is essential to ensure that it has a process in place to deal with a breach at short notice should it occur.

1. The Breach Response Plan below sets out the key issues, which the council has considered in preparing for a data breach.

- (a) The Clerk should be notified immediately of a suspected breach and in the absence of the clerk, the Chairman should be notified.
- (b) The Clerk in consultation with the Chairman will take responsibility with delegated authority to manage the breach. An extraordinary meeting of the Council may be called if required.
- (c) The Clerk will consult other data controllers or contractors as a matter of urgency for any external assistance as necessary and this is covered in the Council's Privacy Policy.
- (d) The Clerk may, depending upon the nature of the breach, need to contact others to identify any actual breach and activate a breach response team if the extent of the breach requires.
- (e) The Council will review its response plan each year, testing the process with others if required.

2. Legal issues

- (a) The Council will maintain legal privilege and confidentiality where required.
- (b) Should a pause of document destruction processes be required, the Clerk will instruct as necessary.
- (c) The Clerk will lead on gathering appropriate evidence and information about the breach.
- (d) The Council if required will contact its external lawyers to manage the investigation and give legal advice.
- (e) The Clerk will ensure that steps to manage the investigation are recorded.
- (f) The Council will contact the Information Commissioners Office ("ICO") and its local law enforcement officer where necessary.
- (g) The Council may take advice from its legal advisers on the legal options available to gather evidence from third parties.
- (h) The Clerk will consult with its legal advisers and/or insurers on potential liabilities to third parties.

3. Data

- (a) Data held by the Council is set out in the Data Audit Log.

(b) The Clerk will ensure that data is held no longer than required.

4. Data subjects

- (a) The Council has in place a Privacy Policy with appropriate notices which are published on its website.
- (b) The Council will provide appropriately worded notifications to data subjects.
- (c) The Council has in place its policies and notices in compliance with GDPR, recognising the potential harm to data subjects should loss of data held by the Council occur.
- (d) The Council is committed to arranging appropriate training for councillors and staff which includes action in the event of a breach.

5. Public Relations

- (a) The Council will consult its legal advisers in dealing with data breaches particularly with pro-active and re-active press statements.
- (b) The Council will put in place arrangements to monitor media reaction as required after any breach.

Changes to this policy

We keep this Security Incident Policy under regular review and we will place any updates on our website. This Policy was last updated in November 2018.

Contact details

Please contact us if you have any questions about this Policy or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

Bishops Lydeard and Cothelstone Parish Council

C/O 37 Stawell Road, Bishops Lydeard, Taunton, TA4 3FA

Email: clerk@bishopslydeardparishcouncil.gov.uk

Adopted by the Council on 14th November 2018

Chairman's Signature: