Sible Hedingham Parish Council Data Breach Policy

Introduction

This Data Breach Policy has been written to enable fast and confident responses to incidents that may occur within Sible Hedingham Parish Council.

Definition

A personal data breach is any event that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes, but is not limited to, a cyber-attack, ransomware infection, lost or stolen device, misdirected email containing personal data, or unauthorised access to council systems with the inclusion of CCTV.

1. Data Responsibilities

Data must be processed securely and measures should be in place for breach detection, investigation and internal reporting. The Clerk acts as the primary officer managing data protection compliance. The Chairman of the parish council is authorised to take over in the Clerk's absence to ensue the 72 hour window for reporting to the ICO is met. The IT Support provider will be on hand to assist with technical breaches.

2. Data Breach Notification and Escalation

In the event of a suspected or confirmed data breach, the following steps must be taken immediately:

- The affected device should be disconnected from the internet and power if a cyber-attack is suspected. The Clerk must contact the IT support provider without delay. The Chairman of the Parish Council must be informed as soon as practicable. If resident or other personal data may be involved, the Clerk must assess whether the breach is likely to result in a risk to the rights and freedoms of individuals.
- Where such a risk exists, the Clerk or Chairman in the Clerk's absence is required under UK GDPR Article 33, to report the breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it. Reports can be made via the ICO website at ico.org.uk/ Where the breach is likely to result in a high risk to affected individuals; those individuals must also be notified without undue delay in accordance with UK GDPR Article 34.

3. **Timescales**

Key actions within the 72 hour reporting window.

- Begin a log to record what happened, who is involved and what is being done about it.
- Write down facts about the incident as they are uncovered: what happened, why, how many people were involved, a timeline of when it happened and what actions have been taken so far.
- Try to contain the breach. Establish what has happened to the personal data affected; if recoverable, do so immediately. Protect those who will be impacted.
- Assess what the risk of harm is to those affected.
- If necessary, act to protect those affected. Give specific and clear advice to people on the steps they can take to protect themselves and what we can do to help.
- Submit the report (if needed.)

We should give specific and clear advice to individuals on the steps they can take to protect themselves and what we can do to help them. Depending on the circumstances, this may include such things as:

- Forcing a password reset;
- Advising individuals to use strong, unique passwords; and
- Telling them to look out for phishing emails or fraudulent activity on their accounts.

4. Recording and Reporting

All breaches, whether reported to the ICO or not, must be recorded in a breach log maintained by the Clerk. The log should include the nature of the breach, the data affected, the action taken and the outcome. The IT support provider will assist with investigation and resolution. All breaches will be reported to Full Council in closed session at the end of the next meeting following the breach. The data breach information shall be kept for up to six years to align with the Limitation Act 1980.

Version 1

Adopted: 1 June 2026

Review: June 2027

Signed by the Chairman: ……

Date …….