****

**Weaverham Parish Council**

**Data Breach Response Plan**

**Introduction**

This Data Breach Response Plan outlines the procedures to be followed in the event of a data breach to ensure a swift and effective response, minimize harm, and comply with legal obligations.

**1. Identification and Reporting**

**1.1 Identifying a Data Breach**

* A data breach can include unauthorized access, loss, theft, or disclosure of personal data.
* Any staff member who becomes aware of a data breach must immediately report it to the Data Protection Officer (DPO) or designated responsible person.

**1.2 Initial Reporting**

* Report the breach to the DPO using the Data Breach Incident Report Form.
* Include details such as the date and time of the breach, type of data involved, how the breach was discovered, and any immediate actions taken.

**2. Containment and Recovery**

**2.1 Immediate Actions**

* The DPO will assess the breach to determine its scope and impact.
* Take immediate steps to contain the breach, such as revoking access, securing systems, or retrieving lost data.

**2.2 Investigation and Recovery**

* Conduct an investigation to determine the cause of the breach and identify affected individuals.
* Implement measures to recover any lost data and restore systems to normal operation.

**3. Risk Assessment**

**3.1 Assessing Risks**

* Evaluate the potential impact of the breach on affected individuals, including risks to their rights and freedoms.
* Consider factors such as the sensitivity of the data, the likelihood of harm, and potential consequences for individuals.

**4. Notification**

**4.1 Internal Notification**

* Inform relevant internal stakeholders, such as council members, about the breach and the steps being taken.

**4.2 External Notification**

* Notify affected individuals if there is a high risk to their rights and freedoms.
* Provide clear information about the breach, the potential impact, and steps individuals can take to protect themselves.
* Notify the Information Commissioner's Office (ICO) within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms.
* If notification is delayed, provide reasons for the delay.

**5. Documentation and Review**

**5.1 Documenting the Breach**

* Maintain a record of the breach, including details of the incident, actions taken, and decisions made.
* Use the Data Breach Incident Report Form to document the breach comprehensively.

**5.2 Review and Improvement**

* Conduct a post-incident review to identify lessons learned and areas for improvement.
* Update policies, procedures, and security measures to prevent future breaches.

**6. Training and Awareness**

**6.1 Staff Training**

* Provide regular training to staff on data protection principles and breach response procedures.
* Ensure staff understand their responsibilities and know how to report a breach.

**6.2 Awareness Campaigns**

* Promote data protection awareness among staff and stakeholders through regular communications and resources.

**Contact Information**

**Data Protection Officer**: Adrian Morgan **Email**:clerk@weaverhampc.co.uk **Phone**: 01606854451