



## **Sarratt Parish Council**

### **Policies and Procedures: GDPR Data Breach Policy**

GDPR defines a personal data breach as 'a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a Data Controller or Processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Sarratt Parish Council takes the security of personal data seriously, computers are password protected and relevant hard copy files are kept in locked cabinets.

#### **1. Consequences of a personal data breach:**

A breach, depending on the circumstances of the breach, can have a range of effects on individuals.

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage.

#### **2. Sarratt Parish Council has a duty to report a breach:**

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual, the Data Protection Officer (DPO) for Sarratt Parish Council and the Information Commissioners Office (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. If the ICO is not informed within 72 hours, Sarratt Parish Council must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, the Parish Council must:

- I. Describe the nature of the breach including the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned.
- II. Communicate the name and contact details of the DPO\*.
- III. Describe the likely consequences of the breach.
- IV. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse affects.

\*DPO contact details: DPO Centre Ltd, 50 Liverpool Street, London, EC2M 7PR.

[advice@dpocentre.com](mailto:advice@dpocentre.com) 0203 797 1289

When notifying the individual affected by the breach, Sarratt Parish Council must provide the individual with (ii)-(iv) above.

Sarratt Parish Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort. However, the ICO must still be informed even if the above measures are in place.

Data Processors have a duty to inform Sarratt Parish Council if they (e.g. payroll provider) become aware of a personal data breach and must notify the Parish Council without undue delay. It is then the Parish Council's responsibility to inform the ICO. It is not the Data Processors responsibility to notify the ICO.

### **3. Records of data breaches**

All data breaches must be recorded whether or not they are reported to individuals.

This record will help to identify system failures and should be used as a way to improve the security of personal data.

### **4. Record of Data Breaches to include:**

- Date of breach.
- Type of breach.
- Number of individuals affected.
- Date reported to ICO/individual.
- Actions to prevent breach recurring.

Date breach should be reported using the ICO online system: <https://ico.org.uk/for-organisations/report-a-breach/>

**Reviewed and adopted:9 March 2021**