Sarratt Parish Council
Policies and Procedures: Personal Data Breach

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. The Council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees and Councillors in the proper performance of their duties.

Where the Council engages third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality, and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Further details can be found in the Council's Information & IT Security Policy.

1. Consequences of a personal data breach:

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.

This means a breach, depending on the circumstances in each case, can have a range of adverse effects on an individual which can include emotional distress and / or physical or material damage.

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 an individual(s), the breach must be reported to the individual(s); the Data Protection Officer (DPO) for the 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, the Council must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, the 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 effects.

*The DPO for Sarratt Parish Council is: DPO Centre Ltd, 50 Liverpool Street, London, EC2M 7PR.

advice@dpocentre.com 0203 797 1289

When it is not possible to provide the information above to the ICO at the same time as reporting the breach, then it must be provided without undue further delay.

3. Data Controller's duty to notify an individual that a data breach has occurred:

GDPR provides that if a personal data breach is likely to result in a "high risk to the rights and freedoms" of an individual(s), the Data Controller must communicate this to the individual(s) "without undue delay".

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

Examples of personal data breaches about which an affected individual(s) would need to be notified include:

- A ransomware attack that results in the Council's electronic personal data being encrypted, back-ups are not available, and the data cannot be restored / made available to the Council
- Personal data is shared electronically with an individual(s) who does not have a legal right to receive such information
- A file containing HR data is left in a public place
- Sensitive personal data is shared on social media
- An old pc containing personal data is donated to another organisation without the data being deleted.
- An ex-employee refuses to return paper or electronic files containing personal data.

GDPR provides that the Council does not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (e.g. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual(s) is no longer likely to materialise; or

- It would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the individual(s) are informed in an equally effective manner.

However, the ICO must still be informed even if the above measures are in place, and the ICO still has the power to request the Data Controller inform the individual(s) if it considers there is a high risk to the rights and freedoms of the individual(s).

4. Data Processor's duty to notify the Data Controller of a personal data breach:

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

5. Records of data breaches

All personal data breaches must be recorded whether or not they need to be reported the individual(s) effected, comprising of the facts relating to the personal data breach, it's effects and the remedial action taken.

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

6. 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.

Personal data breaches should be reported using the ICO online system: https://ico.org.uk/for-organisations/report-a-breach/

Reviewed and adopted: 13 February 2024