Sarratt Parish Council

Policies and Procedures: General Data Protection Regulation (GDPR)

Introduction

Sarratt Parish Council provides many services to local community groups, including sports teams, companies and individuals. In providing services we collect and retain personal data in both written and computer records. The Council also retains information from employees to properly administer areas such as employment records and payroll.

Registration and Data Held

The Council is registered with the Information Commissioners Office (ICO), registration no. Z1299061, and details of the registration can be viewed on the ICO website www.ico.org.uk

Our registration allows us to hold personal data for three purposes, full details of which are contained in our registration.

1. Provision of Local Services.
2. Campaigns, public relations and fund raising.
3. Staff, agent and contractor administration.

Data will be held for an appropriate time, which is set out on our Document Retention Policy, this will vary depending on the reason for which we are holding the data.

Sensitive information as defined in the Data Protection Act, is not held by the Council, other than where necessary for the engagement of employees, elected members (Councillors) and contractors or agency staff.

Purpose

The Council is committed to being transparent about how it collects and uses personal data, and to meeting our data protection obligations. This policy sets out the Council's commitment to data protection, and individuals' rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

This policy applies to the personal data of current and former job applicants, employees, workers, contractors, and former employees, referred to as HR-related personal data. This policy does not apply to the personal data relating to members of the public or other personal data processed for Council business. The Council's General Privacy Notice available on the Council website, refers to the data it is given or collects about individuals and organisations that it works with in order to fulfil the services the Council provides to them.

The Council has appointed the Parish Clerk as the person with responsibility for data protection compliance within the Council. Questions about this policy, or requests for further information, should be directed to them.

Data Controller

The Data Controller for Sarratt Parish Council is the Parish Clerk.

Data Protection Officer

The Data Protection Officer for Sarratt Parish Council is the DPO Centre Ltd.

DPO Centre Ltd
50 Liverpool Street
London
EC2M 7PR
advice@dpocentre.com
0203 797 1289

Definitions

"Personal data" is any information that relates to a living person who can be identified from that data (a 'Data Subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

"Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection Principles

The Council processes HR-related personal data in accordance with the following data protection principles. The Council:

- processes personal data lawfully, fairly and in a transparent manner
- collects personal data only for specified, explicit and legitimate purposes
- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keeps personal data only for the period necessary for processing

- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Council will tell an individual of the personal data it processes, the reasons for processing their personal data, how we use such data, how long we retain the data, and the legal basis for processing in our Privacy Notices.

The Council will not use personal data for an unrelated purpose without telling the individual about it and the legal basis that we intend to rely on for processing it. The Council will not process personal data if it does not have a legal basis for processing.

The Council keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Processing

Personal data

The Council will process personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- it is necessary for the performance of a contract, e.g. a contract of employment (or services); and/or
- it is necessary to comply with any legal obligation; and/or
- it is necessary for the Council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests; and/or
- it is necessary to protect the vital interests of a Data Subject or another person; and/or
- it is necessary for the performance if a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

If the Council processes personal data (excluding special categories of personal data) in line with one of the above bases, it does not require consent. Otherwise, the Council is required to gain consent to process personal data. If the Council asks for consent to process personal data, then we will explain the reason for the request. Individuals do not need to consent or can withdraw consent later.

The Council will not use personal data for an unrelated purpose without telling the individual about it and the legal basis that we intend to rely on for processing it.

Personal data gathered during employment by the Council is held in the employees' personnel files in hard copy and electronic format on HR and IT systems and servers. The periods for which the Council holds HR-related personal data are contained in our Privacy Notices to individuals.

Sometimes the Council will share personal data with contractors and agents to carry out our obligations under a contract with the individual or for our legitimate interests. We require those individuals or companies to keep personal data confidential and secure and to protect it in

accordance with Data Protection law and our policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance with our instructions.

The Council will update HR-related personal data promptly if advised that information has changed or is inaccurate. Employees may be required to provide documentary evidence in some circumstances.

The Council keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Special categories of data

The Council will only process special categories of personal data (see above) on the following basis in accordance with legislation:

- where it is necessary for carrying out rights and obligations under employment law or a collective agreement;
- where it is necessary to protect an employee's vital interests or those of another person where they are physically or legally incapable of giving consent;
- where the data is public;
- where it is necessary for the establishment, exercise or defence of legal claims;
- where it is necessary for the purposes of occupational medicine or for the assessment of an employees working capacity;
- where it is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent;
- where it is necessary for reasons for substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards;
- where is it necessary for reasons of public interest in the area of public health; and
- where is it necessary for archiving purposes in the public interest or scientific and historical research purposes.

If the Council processes special categories of personal data in line with one of the above bases, it does not require consent. In other cases, the Council is required to gain consent to process special categories of personal data. If the Council asks for consent to process a special category of personal data, then we will explain the reason for the request. Individuals do not have to consent or can withdraw consent later.

Individual rights

Data Subjects have a number of rights in relation to their personal data.

Subject Access Requests

Individuals have the right to make a Subject Access Request. If you make a Subject Access Request, the Council will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from yourself;
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the Council has failed to comply with your data protection rights; and
- whether or not the Council carries out automated decision-making and the logic involved in any such decision-making.

The Council will also provide employees with a copy of their personal data undergoing processing. This will normally be in electronic form if they have made a request electronically, unless they agree otherwise.

If you want additional copies, the Council may charge a fee, which will be based on the administrative cost to the Council of providing the additional copies.

To make a Subject Access Request, you should send the request to the Clerk or Chair of the Council. In some cases, the Council may need to ask for proof of identification before the request can be processed. The Council will inform you if we need to verify your identity and the documents we require.

The Council will normally respond to a request within a period of one month from the date it is received. Where the Council processes large amounts of your data, this may not be possible within one month. The Council will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the Council is not obliged to comply with it. Alternatively, the Council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A Subject Access Request is likely to be manifestly unfounded or excessive where it repeats a request to which the Council has already responded. If you submit a request that is unfounded or excessive, the Council will notify you that this is the case and whether or not we will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. You can require the Council to:

- rectify inaccurate data;

- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the Council's legitimate grounds for processing data (where the Council relies on our legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the Council's legitimate grounds for processing data.
- complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

To ask the Council to take any of these steps, you should send the request to the Clerk or Chair of the Council.

Data security

The Council takes the security of HR-related personal data seriously. 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 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.

<u>Impact assessments</u>

Some of the processing that the Council carries out may result in risks to privacy (such as monitoring of public areas via CCTV). Where processing would result in a high risk to your rights and freedoms, the Council will carry out a Data Protection Impact Assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

<u>Data Breaches</u>

The Council have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the Council must take notes and keep evidence of that breach.

If an individual is aware of a data breach they must contact the Clerk or Chair of the Council immediately and keep any evidence, they have in relation to the breach.

If the Council discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of an employee, we will report it to the Information Commissioner within 72 hours of discovery. The Council will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell you that there has been a breach and provide you with information about its likely consequences and the mitigation measures we have taken.

Further details can be found in the Council's Data Breach Policy.

International Data Transfers

The Council will not transfer HR-related personal data to countries outside the EEA.

Employee Responsibilities

Employees are responsible for helping the Council keep their personal data up to date. They should let the Council know if data provided to the Council changes, for example if they move to a new house or change their bank details.

Everyone who works for, or on behalf of, the Council has some responsibility for ensuring data is collected, stored and handled appropriately, in line with the Council's policies.

Employees may have access to the personal data of other individuals and of members of the public in the course of their work with the Council. Where this is the case, the Council relies on them to help meet our data protection obligations to staff and members of the public. Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Council) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to never transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Clerk or Chair of the Council

- to ask for help from the Council's data protection lead if unsure about data protection or if you notice a potential breach or any areas of data protection or security that can be improved upon.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Council's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.

Training

The Council provides training to all individuals about their data protection responsibilities.

Auditing

The Council is periodically audited by the DPO Centre to ensure compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

Reviewed and adopted: 14 March 2023