SHACKLEFORD PARISH COUNCIL

Privacy and Data Protection Policy

Contents

1) Introduction

Shackleford Parish Council (the Council) is committed to fulfilling its obligations under Data Protection law, namely the General Data Protection Regulation (GDPR) and has produced this policy to provide assurance and assist councillors.

The GDPR automatically became UK law on 25th May 2018. The Data Protection Bill will provide additional protections when it becomes law later in the year.

This document is subject to ongoing review in the light of changes in the law and Information Commissioner's guidance.

Key definitions:

- A **controller** determines the purposes and means of processing personal data.
- A **processor** is responsible for processing personal data on behalf of a controller
- A **data subject** means an individual who is the subject of personal information
- **Personal data** means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
- A **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

2) Statement of Data Protection Policy

In order to provide services, the Council needs to collect and use certain types of information. These can include members of the public, current, past and prospective employees, suppliers (such as sole traders) and other individuals.

The Council must also collect and use certain types of information to comply with the law – examples would include Electoral Register information.

The Council will use personal information properly and securely regardless of the method by which it is collected, recorded and used and whether it is held on paper, on a computer or network or recorded on other material such as audio or visual media such as CCTV.

The Council regards the lawful and good management of personal information as crucial to the successful and efficient performance of the Council's functions, and to maintaining confidence. We ensure that the Council treats personal information lawfully and correctly and respects privacy.

To this end, the Council fully endorses and adheres to the principles of Data Protection, as set out in Article 5 of the GDPR.

In addition, the Council will ensure that:

- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;

- everyone managing and handling personal information is appropriately trained to do so;

- anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;

- queries about the handling of personal information are promptly and courteously dealt with; and

- methods of handling personal information are regularly assessed and evaluated.

3) The GDPR Data Protection Principles

The following data protection principles govern the way the Council manages personal information.

1. The law requires that: Personal data must be processed lawfully, fairly and in a manner which is transparent to the data subject;

2. Collection of personal data should be for specified and legitimate purposes;

3. The data the Council collects should be adequate, relevant and limited to what is necessary.

4. The data the Council holds must be accurate and, where necessary, kept up to date;

5. The data the Council holds must be kept in a form which permits identification of data subjects for no longer than is necessary; and

6. The data the Council holds must be processed in a manner that ensures appropriate security of the personal data.

4) The Standards Adopted

The Council will, through appropriate local management and application of corporate criteria and controls:

- observe regulations and codes of practice regarding the fair collection and use of personal information;

- specify the purposes for which personal information is or will be used and through appropriate use of privacy notices;

- collect and process appropriate information to the extent needed to fulfil operational or service needs or to comply with any legal requirements;

- apply checks to determine the length of time information is held regardless of its format. This will be addressed by a corporate Data Retention Schedule and local procedures to establish and keep to appropriate retention periods;

- ensure that the rights of people about whom information is held can be fully exercised under the Act;

- take appropriate technical and organisational security measures to safeguard personal information.

5 Overview of Roles and Responsibilities

Employees and councillors will:

- Ensure they understand how this policy and their local working procedures affect their work.

- Assess the of information they use whilst carrying out their work and whether they have responsibility for any personal information.

- Make sure that they use personal information in accordance with this policy, its associated guidance notes and their local working procedures.

Data Protection Team

The Council uses Guildford Borough Council's Data Protection Officer.

You can report a personal data breach to the Shackleford Parish Clerk at kate.lingard@shacklefordparishcouncil.gov.uk and the DPO at DPO@guildford.gov.uk

Appendix 1

Reference Guide

Breaches of the Data Protection Act
All breaches (suspected breach of confidentiality) should be reported to the Clerk and DPO as soon as they occur. Please refer to the breach notification procedure for full details.

The Information Rights Officer at Guildford Borough Council reports breaches to the Corporate Governance Group on a quarterly basis.

Councillors
In terms of Data Protection, Councillors have three distinct roles:

(1) as a member of a Council committee. In this role, they act for the Council and have the same access rights as a member of staff, subject to the "need to know principle".

(2) Political: they act for their political party or, where independent, their own political agenda, and not for the Council. In this role, the Councillor's access rights are the same as for a political party.

(3) as a representative of one or more constituents: In this role they are acting for the member of the public and not for the Council (in a comparable way to, say, the Citizen's Advice Bureau). The Councillor has the same access rights as the constituents he or she is acting for but must demonstrate that the constituent(s) has given consent for them to act for them.

Couriers
Take care when sending protected information via courier. Encrypted email may be safer. If you cannot avoid using a courier, please follow the procedural guidance on the use of photographers.

Information Security
The Council is responsible for ensuring that personal data which they use or process is kept securely and is not disclosed to any unauthorised person or organisation. Access to personal data should only be given to those who have and can show a business need for access to the data for the purpose of their duties and the principle of least privilege should be applied.

Information Sharing
The Council must only share personal data if it has a lawful basis to do so, where it is necessary to achieve a clear purpose and, with that purpose in mind, it is fair and proportionate to do so. Personal information shared with any Surrey agency must comply with the Surrey Multi Agency Information Sharing Protocol ("Surrey MAISP").

If information is regularly shared with third parties who are not one of the Surrey agencies, Data Sharing Agreements should be in place. However, they are not needed when information is shared in one-off circumstances, but a record of the decision and the reasons for sharing information should be kept.

Retention of records
The Council has a Records Retention and Disposal Schedule which should be referred to when considering how long to keep records for.

The rights of data subjects
Subject to the provisions of the legislation, Councillors, staff and members of the public have the following 'information rights' in relation to their personal data:

to be informed about how and why their personal data is processed;
to access their data;
to rectification of their data;
to erasure of their data;
to restrict processing of their data;
to data portability;
to object to processing of their data; and
not to be subject to fully-automated decision-making including profiling.

1.1 Any information rights requests should be in writing and provide any necessary proof of identification as part of the request.

1.2 The Council aims to respond promptly to these information rights requests and, in any event, within the statutory time limit (normally 30 days).

This policy will take effect from 25 May 2018.