

Littlebury Parish Council Data Protection Policies

Date	Revision
February 2024	Adopted by resolution at Council meeting on 21 February 2024

Contents

Introduction

1. Personal Data
2. The Data Protection Principles
3. Collection and Handling of Personal Data
4. Processing of Personal Data
5. Security of Personal Data
6. Disclosure of Personal Data to Third Parties
7. Subject Access Requests
8. Disposal of Personal Data
9. Breach of any Requirements of the GDPR or Data Protection Act

Littlebury Parish Council Data Protection Policies

Introduction

Littlebury Parish Council collects and uses certain types of personal information about councillors, residents and other individuals who come into contact with the Council. The Council may also be required by law to collect and use certain types of information to comply with statutory obligations. These policies are intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and other related legislation.

The policy applies to both manual files and data stored digitally on computers, other local devices and on cloud based data storage servers.

1. Personal Data

1.1 'Personal data' is defined as information that identifies an individual. It includes, but is not limited to: date of birth, address, phone number, email address, employment history, checks by police and other agencies.

1.2. A sub-set of personal data is known as 'personal sensitive data'. This special category data is information that relates to a person's:

- (i) race or ethnic origin;
- (ii) political opinions;
- (iii) religious or philosophical beliefs;
- (iv) trade union membership;
- (v) physical or mental health;
- (vi) sex life or sexual orientation;
- (vii) genetic or biometric data.

1.3. Personal sensitive data is given special protection, and additional safeguards apply if this information is to be collected and used.

1.4. The Council does not intend to seek or hold personal sensitive data about individuals except:

- (i) where it has been notified of the information;
- (ii) it comes to light via legitimate means; or
- (iii) it needs to be sought and held in compliance with a legal obligation.

2. The Data Protection Principles

2.1. Article 5 of the GDPR sets out six data protection principles which must be followed at all times:

- (i) Personal data shall be processed fairly, lawfully and in a transparent manner;
- (ii) Personal data shall be collected only for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- (iii) Personal data shall be adequate, relevant and limited to what is necessary for the purpose(s) for which it is being processed;
- (iv) Personal data shall be accurate and, where necessary, kept up to date;
- (v) Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that / those purpose(s);
- (iv) Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. Collection and handling of Personal Data

3.1 The Council is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law.

.

3.2. The Council is committed to complying with the data protection principles listed in Paragraph 2 at all times.

3.3. The Council and Clerk will adopt the following procedures when collecting data from individuals. They will:

- (i) inform individuals as to the purpose of collecting any information from them;
- (ii) identify who we will share the information with;
- (iii) indicate how long the Council will retain this information;
- (iv) be responsible for checking the quality and accuracy of the information;
- (v) regularly review the records held to ensure that information is not held longer than is necessary;
- (vi) ensure that when information is authorised for disposal it is done in accordance with the disposal policy outlined in Paragraph 8 ;
- (vii) ensure appropriate security measures to safeguard personal information whether it is held in paper files, on a computer or on a cloud based data storage system;
- (viii) share personal information with others only when it is necessary and legally appropriate to do so;
- (ix) not use personal data for any purpose other than that for which it was originally collected;
(This includes re-use of contact and mailing lists.)
- (ix) set out clear procedures for responding to requests for access to personal information known as subject access requests;
- (x) report any breaches of the GDPR or Data Protection Act to the individual whose data has been compromised and to the Information Commissioner's Office.

4. Processing of Personal Data

4.1. The council will not unnecessarily undertake the processing of personal data, except where

- (i) the individual has given consent that is specific to the particular type of processing activity;

(ii) the processing is necessary for the performance of a legal obligation to which the Council is subject;

(iii) the processing is necessary for entering into or performing a contract, between the individual and the Council;

(iv) the processing is necessary to protect the vital interests of the individual or another person.

5. Security of Personal Data

5.1. The Council will take reasonable steps to ensure that the Clerk and councillors will have access to personal data only where it is necessary for them to carry out their duties.

5.2. The Council will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons. This will include the following;

(i) where the personal data is in hard copy it will be securely kept in a locked cabinet or room to which only those authorised to access the data have access;

(ii) where the data is stored in electronic form it will be on a device which has up to date security software installed and is protected by password which is accessible only to those authorised to access the data;

(iii) where the data is stored on a remote device or server it will be protected by a password known only to those authorised to access the data.

6. Disclosure of Personal Data to Third Parties

6.1. The Council may receive requests from third parties to disclose personal data it holds about staff, councillors or other individuals. The Council will not disclose personal data to third parties except:

(i) to give a confidential reference relating to a current or former employee, with the consent of the individual concerned;

(ii) for the prevention or detection of crime;

(iii) for the assessment of any tax or duty;

(iv) when it is necessary to exercise a right or obligation conferred or imposed by law;

(v) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

(vi) for the purpose of obtaining legal advice;

6.2. All requests for the disclosure of personal data must be sent to the Clerk who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

7. Subject Access Requests

7.1. Anybody who makes a request to see any personal information held about them by the Council is making a subject access request. All information relating to the individual, whether that held in electronic or paper files, should be considered for disclosure.

7.2. A subject access request must be made in writing to the Clerk who may ask for any further information reasonably required to locate the information.

7.3. An individual also has the right to;

(i) object to the processing of their personal data and to block or restrict the processing;

(ii) request the rectification of inaccurate data;

(iii) have incomplete information completed by providing the missing data.

7.4. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

(i) where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

(ii) where consent is withdrawn and there is no other legal basis for the retention or processing of the data;

(iii) the individual believes the legal conditions for processing cannot be met.

7.5. All requests under Paragraphs 7.1 to 7.4 shall be addressed by the Clerk and a response provided in writing to the individual within 20 days of the receipt of the request.

7.6. Where the Clerk has reason to dispute the request the matter will be referred to the Chair and if appropriate to the full Council for resolution.

7.7. The Council's response to any dispute in Paragraph 7.7 shall be notified to the individual along with reasons for the decision within 20 days of receipt of the request.

8. Disposal of Personal Data

8.1. The Council shall not retain personal data for longer than is necessary for the purpose for which it was acquired.

8.2. All personal data will be destroyed no later than 5 years after it was acquired unless there is an ongoing need to retain it.

8.3. The Clerk will review on an annual basis all personal data held by the Council to assess whether it needs to be retained. The Clerk will keep a permanent record of this review and inform the Council on its completion.

8.4. Personal data which meets the criteria in Paragraphs 8.1 and 8.2. will be permanently destroyed as follows;

(i) data stored in hard copy will be shredded using a cross cutting device or professional shredding service;

(ii) data stored electronically will be permanently deleted from all devices and servers on which it is stored.

9. Breach of any Requirements of the GDPR or Data Protection Act

9.1. Any and all breaches of the GDPR, the Data Protection Act, and any of the policies in this document must be reported immediately to the Chair, who will decide whether to bring it to the attention of the full Council.

9.2. The Chair in conjunction with the Clerk shall assess;

- (i) the extent of the breach;
- (ii) the risks to the data subjects as a consequence of the breach;
- (iii) any security measures in place that will protect the information;
- (iv) any measures that can be taken immediately to mitigate the risk to the individuals.

9.3. Unless the Chair concludes that there is unlikely to be any risk to individuals from the breach:

- (i) he/she will notify the full Council;
- (ii) the breach must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Council.

9.4. The Council will co-operate fully with the Information Commissioner's Office to provide all requested information about the breach and to enable any subsequent enquiry.