DATA PROTECTION POLICY

Winterbourne Parish Council is committed to the protection of personal data and will always comply with obligations under applicable data protection law including the Data Protection Act 1998 (DPA), which covers both electronic data and data held on manual records.

It is the responsibility of each elected member and every employee, worker and volunteer to be aware of their individual and collective responsibilities under the Act and to make sure they comply with its provisions.

Deliberate breaches of this policy will be considered as gross misconduct. Individuals, as well as the Parish Council, can be prosecuted for breaches of the Data Protection Act.

The Parish Council will be open about the type and extent of personal data it holds. It will keep the minimum amount of personal information needed to perform its duties; it will hold that information securely, use it only for appropriate purposes and not disclose it without proper authority.

Definitions

Personal Data: is information that can identify a living individual. This includes Sensitive Data (see below), names, addresses, photographs, National Insurance numbers, bank account details – these are just a few examples and the list is endless.

Sensitive Data: is personal data relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union movement members, health, sexual orientation, criminal proceedings or convictions.

Processing: means any operation carried out by the Parish Council or its staff on Personal Data (e.g. collection, storage, disclosure, transfer and deletion).

The Rules of Fair Processing - Key Principles

The DPA contains 8 principles that apply to all personal data processing. Personal data must always be:
1 Fairly and lawfully processed.
2 Processed for clearly identified purposes that have been notified to individuals who give the Parish Council data.
3 Relevant and not excessive for the purpose told to individuals.

4 Accurate and where necessary, kept up to date.
5 Not kept for longer than is necessary.
6 Processed in line with the individual's rights.
7 Secure.
8 Not transferred to countries without adequate protection.

Principle 1-3 Processing Personal Data

Processing personal data may only be carried out where one of the following conditions has been met;
• The individual has given his or her consent to the processing;
• The processing is necessary for the performance of a contract with the individual;
• The processing is required under a legal obligation;
• The processing is necessary to protect the vital interests of the individual;
• The processing is necessary to carry out public functions;
• The processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual)

Principle 1-3 Processing Sensitive Data

Processing sensitive data can only be processed under strict conditions which include;
• Having the explicit consent of the individual;
• Being required by law to process the data for employment purposes;
• Needing to process the information in order to protect the vital interests of the data subject or another;
• Dealing with the administration of justice or legal proceedings

Sensitive Data will not be processed fairly and lawfully unless it is processed with the explicit consent or where required under one of the following circumstances:
▪ For employment purposes.
▪ To protect vital interest of the individual or another.
▪ For the administration of justice or legal proceedings.

Principle 4

All staff, workers and volunteers must make every effort to ensure that any personal data entered on to the computer system is recorded accurately. The Data Protection Act also extends to manual records if they are or form part of a "relevant filing system". Staff, workers and volunteers will be responsible for updating records as and when notification is received from the individual/contractor, agency or other of a change in their personal details. When the Parish Council is notified of bereavement, the individual's details must be deleted immediately.

Principles 5 -7

Staff, workers and volunteers must take security measures to safeguard personal data. This includes technical measures (e.g. password protection of the computer system) and organisational measures (e.g. burglar alarms and door locks). The measures are designed to prevent any unauthorised access to, or disclosure of, personal data.

Personal Data Requests

Winterbourne Parish Council will provide any person requesting it in the proper manner a response stating whether or not the Parish Council holds personal information about that individual and, if so, the opportunity to see the information and have it corrected or deleted if appropriate. A person may only request details about themselves and no other person. The Parish Council is entitled to levy a charge for this service.

A person about whom information is held is entitled (subject to a fee) to be informed whether any information is held on him/her to;
• A description of the data; and
• A copy of the information in an intelligible form.

The data subject is also entitled to request and receive information pertaining to;
• The purpose for which the data is being held;
• The recipients or classes of recipients to who it may be disclosed; and
• The source of the data.

Councillors' Data Protection responsibilities

Councillors must inform the Information Commissioner's office (ICO) if they process personal data on computers for purposes other than council business (e.g. for ward casework).

Paper files/manual records

The Data Protection Act 1988 includes manually processed information in the definition of "data" and relates to information which forms part of a "relevant filing system". The data must be capable of being accessed by reference to the individual or criteria relating to the individual. For more information on the Data Protection Act, the Information Commissioner's website provides useful guidance www.informationcommissioner.gov.uk

Date of adoption of policy: 6 March 2023

Date of next review: 6 March 2025