

Data Protection Policy

The Data Protection Policy

Weston in Gordano Parish Council [the Parish Council] recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as simple as a name and address.

Personal data is any data which can be used to identify a natural living person.

General Data Protection Regulations (GDPR)

This policy applies to all councillors, employees, volunteers, and any third party or contractor handling personal data on behalf of the Parish Council.

The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The GDPR applies to anyone holding personal information about people, electronically or on paper. The Parish Council has also notified the Information Commissioner that it holds personal data about individuals (Registered as a data Controller).

When dealing with personal data, the Parish Council staff and members must ensure that:

- **Data is processed fairly, lawfully and in a transparent manner**
This means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.
- **Data is processed for specified purposes only**
This means that data is collected for specific, explicit and legitimate purposes only.
- **Data is relevant to what it is needed for**
Data will be monitored so that too much or too little is not kept; only data that is needed should be held.
- **Data is accurate and kept up to date and is not kept longer than it is needed**
Personal data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.
- **Data is processed in accordance with the rights of individuals**
Individuals must be informed, upon request, of all the personal information held about them.
- **Data is kept securely**
The Clerk acts as the Council's primary contact for data breaches, maintains the breach log, and is responsible for reporting incidents to the ICO where required, in accordance with the Council's Data Breach Policy. There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Storing and accessing data

The Parish Council recognises its responsibility to be open with people when taking personal details from them. This means that staff must be honest about why they want a particular piece of personal information.

The Parish Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. Councillors may also handle personal data during their duties, including resident correspondence, planning comments, complaints, volunteer and event information, and employment-related data where appropriate. These will be securely kept at the Parish Council Office and are not available for public access.

All data stored on the Parish Council Office computers are password protected. Councillors and staff who access Council information on personal devices must ensure those devices are password-protected and that any personal data is stored securely and deleted when no longer required. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of Councils document retention policy, it will be shredded or securely deleted from the computer. Records relating to data breaches will be retained securely for a minimum of six years, in accordance with the Council's Document Retention Policy.

The Parish Council is aware that people have the right to access any personal information that is held about them. Data Subject Access Requests (DSARs) can be submitted verbally (in person, on the phone) or in writing (hard copy, email or social media). If a person requests to see any data that is being held about them, the DSAR response must detail:

- How and to what purpose personal data is processed
- The period the Parish Council intend to process it for
- Anyone who has access to the personal data

The response must be sent within 30 days and should be free of charge.

If a DSAR response includes personal data of other individuals, the Parish Council must not disclose the personal information of the other individuals. The other individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the Subject.

Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests.

Please see "Data Subject Access Request Procedure" for more details.

Confidentiality

The Parish Council members and staff must be aware that when complaints or queries are made, they must remain confidential unless the data subject gives permission otherwise. When handling personal data, this must also remain confidential.

Version number	Purpose/change	Author	Date
0.1	Initial draft	LSS	05/03/18
0.2	Review and Update	NH	June 2025
0.3	Approved	LS	Nov 2025