

Bolton by Bowland, Gisburn Forest & Sawley Parish Council

DATA PROTECTION POLICY

1. Introduction

Bolton by Bowland, Gisburn Forest & Sawley Parish Council has a responsibility under the General Data Protection Regulations 2018 to hold, obtain, record, use and store all personal data relating to an identifiable individual in a secure and confidential manner. This Policy is a statement of what the Parish Council does to ensure its compliance with the Act.

The Data Protection Policy applies to all Parish Council employees, councillors, volunteers, residents, members of the public and contractors. The Policy provides a framework within which the Parish Council will ensure compliance with the requirements of the Act and will underpin any operational procedures and activities connected with the implementation of the Act.

2. Background

The General Data Protection Regulations 2018 governs the handling of personal information that identifies living individuals directly or indirectly and covers both manual and computerised information. It provides a mechanism by which individuals about whom data is held (the “data subjects”) can have a certain amount of control over the way in which it is handled.

Some of the main features of the Act are:

- All data covered by the Act must be handled in accordance with the Six Data Protection Principles (see Appendix 1).
- The person about whom the information is held (the Data Subject) has various rights under the Act including the right to be informed about what personal data is being processed, the right to request access to that information, the right to request that inaccuracies or incomplete data are rectified, and the right to have personal data erased and to prevent or restrict processing in specific circumstances. Individuals also have the right to object to processing based on the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling); and processing for the purposes of scientific/historical research and statistics. There are also rights concerning automated decision making (including profiling) and data portability.
- Processing of special categories of data must be done under a lawful basis. This data includes information about race, ethnic origin, political persuasion, religious belief, trade union membership, health and sexual orientation.
- The General Data Protection Regulations deal with criminal offence data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.
- There is a principle of accountability of data controllers to implement appropriate technical and organisational measures that include internal data protection policies and procedures, staff training and awareness of the requirements of the Regulations, internal audits of processing activities, maintaining relevant documentation on processing activities and implementing measures that meet the principles of data protection by design and data protection by default, including data minimisation, transparency, and creating and improving security features on an ongoing basis.
- Data protection impact assessments are carried out where appropriate as part of the design and planning of projects, systems and programmes.

- Data controllers will have written contracts in place with all data processors and ensure that processors are only appointed if they can provide 'sufficient guarantees' that the requirements of the Regulations will be met and the rights of data subjects protected.
- Data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office within 72 hours of the Parish Council becoming aware of the breach. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Parish Council will notify those individuals concerned directly.
- The Information Commissioner is responsible for regulation and issue notices to organisations where they are not complying with the requirements of the Regulations. He /she also has the ability to prosecute those who commit offences under the Regulations and to issue fines.

3. Policy Statement

The Parish Council is committed to ensuring that personal information is handled in a secure and confidential manner in accordance with its obligations under the General Data Protection Regulations 2018 and professional guidelines. The Parish Council will use all appropriate and necessary means at its disposal to comply with the General Data Protection Regulations 2018 and associated guidance.

4. Roles and Responsibilities

4.1. Parish Council

The Parish Council will be responsible for ensuring that the organisation complies with its responsibilities under the General Data Protection Regulations 2018 through monitoring of activities and incidents. The Parish Council will also ensure that there are adequate resources to support the work outlined in this policy to ensure compliance with the General Data Protection Regulations 2018.

4.2. All Staff and Councillors

All staff and councillors will ensure that:-

- Personal information is treated in a confidential manner in accordance with this and any associated policies. This is in line with the Parish Council's Code of Conduct & Standing Orders regarding matters of confidentiality, which may be viewed on the Parish Council website www.tsbparish.org.uk.
- The rights of Data Subjects are respected at all times.
- Privacy notices will be made available via the Village Notice Boards and on the Parish Council website to inform individuals how their data is being processed.
- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose.
- Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information.
- Personal information held within applications, systems, personal or shared drives is only accessed in order to carry out work responsibilities.
- Personal information is recorded accurately and is kept up to date.
- They appropriately handle any subject access requests and/or requests in relation to the rights of individuals.
- They appropriately handle actual or potential breaches of the General Data Protection Regulations 2018 as soon as the breach is discovered.

It is the responsibility of all staff and Parish Councillors to ensure that they comply with the requirements of this policy and any associated policies or procedures.

4.3. Contractors and Employment Agencies

Where contractors are used, the contracts between the Parish Council and these third parties should contain mandatory information assurance clauses to ensure that the contract staff are bound by the same code of behaviour as Parish Council members of staff and Parish Councillors in relation to the General Data Protection Regulations 2018

4.4. Volunteers

All volunteers are bound by the same code of behaviour as Parish Council members of staff and Parish Councillors in relation to the General Data Protection Regulations 2018.

5. Records Management

Good records management practice plays a pivotal role in ensuring that the Parish Council is able to meet its obligations to provide information, and to retain it, in a timely and effective manner in order to meet the requirements of the Regulations. All records should be retained and disposed of in accordance with the Parish Council Retention Schedule.

6. Consent

The Parish Council will take all reasonable steps to ensure that service users, members of staff, volunteers, and contractors are informed of the reasons the Parish Council requires information from them, how that information will be used and who it will be shared with. This will enable the Data Subject to give explicit informed consent to the Parish Council handling their data where the legal basis for processing is consent.

Should the Parish Council wish to use personal data for any purpose other than that specified when it was originally obtained, the Data Subject's explicit consent should be obtained prior to using the data in the new way unless exceptionally such use is in accordance with other provisions of the Regulations.

Should the Parish Council wish to share personal data with anyone other than those recipients specified at the time the data was originally obtained, the Data Subject's explicit consent should be obtained prior to sharing that data. Failure to do so could result in a breach of confidentiality.

7. Accuracy and Data Quality

The Parish Council will ensure that all reasonable steps are taken to confirm the validity of personal information directly with the Data Subject.

All members of staff and Parish Councillors must ensure that service user personal information is checked and kept accurate and up to date on a regular basis.

Where a member of the public exercises their right for their data to be erased, rectified, or restricted, or where a member of the public objects to the processing of their data the appropriate procedures will be followed.

8. Data Protection Impact Assessments

A Data Protection Impact Assessment is a process which helps to assess privacy risks to individuals in the collection, use and disclosure of information. They must be carried out at the early stages of projects and are embedded in to the Parish Council's decision-making process.

9. Providers

The Parish Council must have written contracts in place with all suppliers who process personal data on behalf of the Parish Council as "data processors". The Parish Council will ensure that processors are only appointed if they can provide 'sufficient guarantees' through the procurement process that the requirements of the Regulations will be met and the rights of Data Subjects protected.

10. Complaints

Any expression of dissatisfaction from an applicant with reference to the Parish Council's handling of personal information will be treated as a complaint, and handled under the Parish Council's Complaint's Procedures.

Should the complainant remain dissatisfied with the outcome of their complaint to the Parish Council, a complaint can be made to the Information Commissioner's Office who will then investigate the complaint and take action where necessary.

11. Security and Confidentiality

All staff and Parish Councillors must ensure that information relating to identifiable individuals is kept secure and confidential at all times. The Parish Council will ensure that its holdings of personal data are properly secured from loss or corruption and that no unauthorised disclosures of personal data are made.

The Parish Council will ensure that information is not transferred to countries outside the European Economic Area (EEA) unless that country has an adequate level of protection for security and confidentiality of information which has been confirmed by the Information Commissioner.

12. Rights of Data Subjects

Individuals wishing to request their information as a Subject Access Request should contact the Data Controller of the Parish Council, who will arrange for the information to be processed in accordance with the General Data Protection Regulations.

Individuals should also make requests in writing to the Parish Council if they wish to exercise their other rights under the legislation.

APPENDIX 1

DATA PROTECTION PRINCIPLES

First Principle

Processed lawfully, fairly and in a transparent manner in relation to individuals;

Second Principle

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

Third Principle

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Fourth Principle

Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Fifth Principle

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

Sixth Principle

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.