



To operate, Brize Norton Parish Council and its Sub-Committees needs to collect and use personal information about its employees, elected members, parishioners, suppliers and others with whom it communicates. We have a responsibility to ensure that this personal information is handled in accordance with statutory requirements; however, it is collected, recorded and used; whether on paper, in a computer, or in other material. The Council and its Sub-Committees will follow the eight Data Protection Principles of the Data Protection Act 1998 to ensure that this personal information is:

1. Processed fairly and lawfully and such processing must comply with at least one of a set of specified conditions contained in the 1998 Act. Additional conditions apply to sensitive personal data;
2. Obtained only for one or more specified and lawful purpose, and shall not be processed in any manner incompatible with the purpose(s);
3. Adequate, relevant and not excessive in relation to those purpose(s) for which it is processed;
4. Accurate, and where necessary kept up-to-date;
5. Not kept for longer than is necessary for the purpose(s) for which it was processed;
6. Processed in line with the rights of data subjects under the Act;
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. Not transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data protection is a responsibility shared by all employees, elected members and sub-committee members but **The Clerk to the Council** has overall responsibility for ensuring the effective implementation of this Policy. He/she will report to the Council on all matters relating to data protection and:

- Review, renew and amend the Council's notification.
- Monitor compliance with established policies and standards.
- Provide general advice and guidance on data protection matters.
- Update this policy.

Implementation of the data protection principles mean that:

- Where the Council and/or its Sub-Committees requires the consent of an individual to hold/process information about him/her, they will be informed of all the purposes(s) for which the data is to be used by the processor i.e. the Council.
- Personal data will only be used for the purpose(s) advised to the individual at the time they supplied the information.

- As far is possible, personal data held about an individual, including opinions and/or statements, will be kept up to date and accurate. It will be adequate, relevant and not excessive in relation to the purpose(s) for which it is held. Once it is no longer relevant it will be destroyed.
- Personal data will not be disclosed to unauthorised personnel – depending on the nature of the information these can include people outside the Council, as well as Council employees and Elected Members.
- Any Freedom of Information (Fol) request by an individual for information about himself will be handled as a Data Subject Access Request. Where a request is made that specifically asks for information about a third party, or where responding to a request would involve disclosure of personal information about a third party, we will apply Data Protection Principles when considering disclosure. Relevant physical and electronic security measures will be taken to ensure that personal data is kept secure at all times.

Data Subject Notices

Everyone has the right on written request (irrespective of age) to:

1. See a copy of information held about them (for the payment of a fee of £10).
2. Prevent processing likely to cause damage or distress.
3. Prevent processing for direct marketing purposes.
4. Request a review of an automated decision.
5. Apply to the Court for rectification, blocking, erasure and destruction of personal information.
6. Request an assessment by the Information Commissioner's Office.

Where the Council receives such a request the Clerk will deal with it as soon as possible to ensure a response is sent within 21 days.

Sensitive Personal Data

Where sensitive personal information is held or used, i.e. information relating to an individual's race, political opinions, religion, trade union membership. 'physical or mental health condition', sexual life and criminal proceedings or convictions; consent for processing will be obtained unless the purpose is covered in Section 3 of the Data Protection Act 1998.

Training

Everyone managing and/or handling personal information will be appropriately trained.

Evaluation and Review

This policy will be reviewed by the Clerk to the Council on a regular basis to ensure that it continues to:

- Meet the needs of the staff of the Council
- Be practical to implement
- Embody new developments in good practice and technology

Signed

 CHAIRMAN

Date 4/12/2017