BURGHFIELD PARISH COUNCIL
Clerk: Cally Morris, PO Box 7381, Reading, RG1 9XP
Tel: 0118 983 1748
Email: clerk@burghfieldparishcouncil.gov.uk
Website: www.burghfieldparishcouncil.gov.uk

DATA PROTECTION POLICY

1. Introduction

The General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018) amend and update the existing framework of rights and duties which safeguard personal data. Personal data is information about a living individual (a data subject) who can be identified from such data and should be broadly interpreted as it encompasses not only names and addresses but can include photographs, email addresses, and digital data such as IP addresses and cookie identifiers. This legal framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal data.

Burghfield Parish Council is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with the GDPR and the DPA 2018. The Council has established the following policy to support this commitment. It is the personal responsibility of all employees, Members, contractors, agents, and anyone else processing information on behalf of the Parish Council to comply with this policy. This policy continues to apply to employees and individuals even after their relationship with the Council ends.

Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation. All incidents will be investigated, and action may be taken by the Council's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and/or criminal action being taken.

2. Data Protection Principles (Article 5)

The GDPR are underpinned by a set of seven common-sense Principles which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing, and deleting personal data.

- Processing must be lawful, fair, and transparent.
- The purposes for which data is processed must be specific, explicit, and legitimate.
- Data which is processed must be limited to what is adequate and relevant. If depersonalised information is sufficient, personal data must not be collected.
- Data which is processed must be accurate and kept up to date.
- Data must be retained no longer than is necessary.
- Data must be kept securely and protected against unauthorised access, theft, or loss.
- The Data Controller must be responsible for and able to demonstrate their compliance with these Principles (accountability).

3. Lawful Basis for Processing (Article 6(1))

When Burghfield Parish Council processes personal data, it must have a lawful basis for doing so. Processing is only lawful if at least one of the conditions below is met.

- Consent – which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes, signified by a statement or a clear affirmative action.

- Contract – with the data subject. Examples might be data processed for a contractual obligation such as hall hire, cemetery records, or allotment rentals.
- Legal obligation – of the Data Controller. An example might be disclosing salary details of employees to HMRC. It also covers dealing with complaints, planning matters, and FoI enquiries.
- Vital interests – of the data subject or someone else. An example might be providing information about elderly residents to local emergency services in a civil emergency such as a fire or flood.
- Public Interest – processing carried out for the performance of a task in the public interest, which includes the exercise of a function conferred on a person by an enactment or rule of law and an activity that supports or promotes democratic engagement – an example is canvassing on behalf of elected members.

Because in most cases the lawful basis for processing is 'informed consent', the data subject (the person who the information is about) must be told, unless this is obvious to them, which organisation(s) they are giving their information to; what their information will be used for; who it may be shared with; how it will be safeguarded and how long it will be held, as well as anything else that might be relevant e.g., the consequences of that use. A formal notice known as a Privacy Notice can be used to provide this information. If the personal data is collected for one purpose, it must not subsequently be used for a different and unconnected purpose without the data subject's consent (unless there is another lawful basis for using the information).

4. Special Categories of Personal Data (Article 9)

The GDPR identifies 'Special Categories of Personal Data' which require higher levels of protection and consent. Burghfield Parish Council will process these categories in compliance with the provisions of the GDPR. Special Categories of Personal Data include: Racial or ethnic origins, Political opinions, Religious or philosophical beliefs, Trade-Union membership, Genetic or biometric data, Health data, and Sexual orientation or sex life.

5. Access to and Use of Personal Data

Access to and use of personal data held by the Council is only permitted by employees, Members, contractors, agents, and anyone else processing information on behalf of the Parish Council for the purpose of carrying out their official duties. Processing for any other purpose is prohibited. Deliberate unauthorised access to, copying, disclosure, destruction, or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal offence and/or disciplinary offence.

6. Disclosing Personal Data

Personal data must not be disclosed to anyone internally or externally unless the person disclosing the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information. If personal data is disclosed to another organisation or person outside of the Parish Council, the disclosing person must identify their lawful basis for the disclosure and record their decision. This should include a description of the information disclosed; the name of the person and organisation to which the information was disclosed; the date; the reason for the disclosure; the lawful basis.

7. Accuracy and Relevance

It is the responsibility of those who receive personal information to ensure, as far as possible, that it is accurate and up to date. Personal data should be checked at regular intervals to ensure that it is still accurate. If the information is found to be inaccurate, steps must be taken to rectify it. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous, and professionally worded

8. Retention and Disposal of Personal Data

Personal data should be held only for as long as it is required for the purpose for which it was collected. To facilitate this, Burghfield Parish Council holds a Record Retention Schedule/Record Management Policy which provides guidance on prescribed retention periods for the personal data and other information it holds. Personal data must be deleted or destroyed in a secure fashion.

9. Individual Rights

Under GDPR, individuals have several rights regarding their personal data, including:

- Right to transparency (Privacy Notices and other information about how personal data is processed).
- Right of access (subject access requests).
- Right to rectification (correction of inaccurate data).
- Right to erasure (the 'right to be forgotten').
- Right to object to processing (in cases of direct marketing).
- Right to data portability (requesting transfer of data to another data controller).
- Right to withdraw consent at any time where processing is based on consent.

10. Subject Access Requests (SAR's)

Individuals have the right to make a SAR to find out what data is held about them. Requests must be made in writing or verbally and the council has one calendar month to respond. The council may charge a fee based on the administrative cost for additional copies. Verification of identity may be required before processing the request.

11. Data Breaches

The Council has robust measures in place to minimise and prevent data breaches. Any breach must be reported to the Clerk or Chairman immediately. Serious breaches that pose a risk to individuals' rights and freedoms must be reported to the ICO within 72 hours.

12. Data Security

Burghfield Parish Council takes the security of personal data seriously and has implemented appropriate technical and organisational measures to protect against loss, accidental destruction, misuse, or disclosure. Third parties processing data on behalf of the council must follow these security measures and are subject to written agreements ensuring their compliance.

13. Training and Awareness

Regular training for staff and councillors on data protection principles and practices is essential to ensure ongoing compliance with this policy and data protection legislation.

14. Roles and Responsibilities

The Clerk acts as the Data Protection Officer (DPO) responsible for informing and advising the Parish Council on their data protection obligations, monitoring compliance, and acting as the contact point for the ICO. The DPO is provided with the necessary resources and access to personal data to perform these tasks.

Burghfield Parish Council is committed to ensuring compliance with GDPR and DPA 2018 by adhering to this Data Protection Policy and continuously reviewing and updating its practices.

15. Registration

Parish and Town Councils are required to register with the Information Commissioner in order to process personal data. Burghfield Parish Council is registered to process personal data and the Registration Reference is **Z6495003.**

Burghfield Parish Council
Clerk: Cally Morris
PO Box 7381
Reading
RG1 9XP

Tel: 0118 983 1748
Email: clerk@burghfieldparishcouncil.gov.uk
Website: www.burghfieldparishcouncil.gov.uk