Downend & Bromley Heath Parish Council –

Information and General Data Protection Policy

1. Introduction

1.1 In order to conduct its business, services, and duties, the Parish Council processes a wide range of data related to its own operations and some handled on behalf of partners. Broadly, this data can be classified as follows:

1.1.1 Data shared publicly about the services it offers, its operations, and other information that must be made available to the public.
1.1.2 Confidential information and data that is not yet public, such as ideas or policies in development.
1.1.3 Confidential information about other organisations due to commercial sensitivity.
1.1.4 Personal data concerning current, past, and potential employees, Councillors, and volunteers.
1.1.5 Personal data concerning individuals who contact the Council for information, to access services or facilities, or to make a complaint.

1.2 The Parish Council will adopt procedures to responsibly manage all data it handles, respecting the confidentiality of both its own data and that of partner organisations and the public. In some cases, there may be contractual obligations towards confidential data, in addition to specific legal responsibilities for personal and sensitive information under data protection legislation.

1.3 The Parish Council will periodically review and revise this policy based on experience, feedback from data subjects, and guidance from the Information Commissioner's Office.

1.4 The Parish Council will be transparent about its operations and work closely with public, community, and voluntary organisations. Therefore, it will make available all non-personal and non-confidential information to partners and members of the parish communities. A list of information routinely available can be found in the Parish Council's Publication Scheme, which aligns with the statutory model publication scheme for local councils.

---

2. Protecting Confidential or Sensitive Information

1.5 The Parish Council recognises that at times, it must process sensitive and personal information about employees and the public. It has therefore adopted this policy not only to meet legal obligations but also to ensure high standards of data protection.

1.6 The General Data Protection Regulation (GDPR), which became law on 25 May 2018, seeks to strike a balance between the rights of individuals and the interests of organisations, such as the Parish Council, with legitimate reasons for using personal information.

1.7 This policy is based on the premise that personal data must be:

1.7.1 Processed fairly, lawfully, and in a transparent manner concerning the data subject.
1.7.2 Collected for specified, legitimate purposes and not further processed in a way that is incompatible with those purposes.
1.7.3 Adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
1.7.4 Accurate and, where necessary, kept up to date.
1.7.5 Kept in a form that permits identification of data subjects only for as long as necessary for processing.
1.7.6 Processed securely, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

---

3. Data Protection Terminology

Data subject – The individual whose personal data is being processed. This could be an employee, prospective employee, associate, or anyone transacting with the Parish Council.
Personal data – Any information relating to a natural person or data subject that can be used to identify them directly or indirectly, including names, photos, addresses, email addresses, bank details, social media posts, and IP addresses.
Sensitive personal data – Information about racial or ethnic origin, political opinions, religious beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data, or details related to offences or alleged offences.
Data controller – The person (e.g., the Parish Council) who determines the purposes for which and how personal data is processed.
Data processor – A person or entity (other than the data controller's employees) who processes personal data on behalf of the data controller.
Processing information/data – Includes operations such as obtaining, recording, organising, altering, retrieving, disclosing, and destroying personal data, regardless of the technology used.

---

4. When Will the Parish Council Process Personal Information?

1.8 The Parish Council processes personal data to:

1.8.1 Fulfil its duties as an employer, including complying with employment contracts and legal obligations.
1.8.2 Pursue its legitimate interests as a public body by fulfilling contractual terms and maintaining legally required information.
1.8.3 Monitor activities, including equality and diversity.
1.8.4 Manage business premises, including security.
1.8.5 Assist regulatory and law enforcement agencies.

1.8.6 Update and maintain records about Councillors, employees, partners, and volunteers.
1.8.7 Handle inquiries, service requests, or complaints from the public.
1.8.8 Conduct surveys, censuses, and questionnaires for the Parish Council's objectives.
1.8.9 Perform research, audits, and quality improvement to support the Parish Council's objectives.
1.8.10 Carry out administrative functions of the Parish Council.

---

5. Conditions for Processing Personal Data

1.10 The Parish Council will ensure at least one of the following conditions is met for personal information to be considered fairly processed:

1.10.1 The individual has consented to the processing.
1.10.2 Processing is necessary for the performance of a contract or agreement with the individual.
1.10.3 Processing is required by law.
1.10.4 Processing is necessary to protect the individual's vital interests.
1.10.5 Processing is necessary to carry out public functions.
1.10.6 Processing is necessary to pursue the legitimate interests of the Parish Council or third parties.

---

6. Sensitive Personal Information

1.11 Extra care is taken when processing sensitive personal data, ensuring that at least one of the following conditions is met:

1.11.1 Explicit consent of the individual.
1.11.2 Processing required by law for employment purposes.
1.11.3 Processing necessary to protect the vital interests of the individual or another person.

---

7. Data Protection Responsibilities

The Parish Council, as a corporate body, has ultimate responsibility for ensuring compliance with data protection laws. Day-to-day responsibility is delegated to the Clerk:

- Email: clerk@dbhparishcouncil.co.uk
- Phone: 0117 9567001
- Correspondence: The Parish Clerk, Parish Office, Downend Library, Buckingham Gardens, Downend, Bristol BS16 5TW

The Parish Council may, in the future, appoint an external Data Protection Officer to ensure compliance.

8. Information Security

1.18 The Parish Council ensures the security of personal data, protecting it from unauthorised access, loss, manipulation, falsification, destruction, or unauthorised disclosure. This is achieved through appropriate technical measures and policies.

1.19 Personal data will only be retained for the purpose for which it was collected and only for as long as necessary, after which it will be deleted.

---

9. Rights of Data Subjects

1.21 **Access to Information**: Individuals have the right to request access to the information we hold about them.
1.22 **Correction**: If an individual believes the information we hold is incorrect, they can contact us to have it updated.
1.23 **Deletion**: Individuals may request the deletion of their information.
1.24 **Right to Object**: Individuals can object to the processing of their data if they believe it is not being used for its intended purpose.
1.25 The Parish Council does not use automated decision-making or profiling of individual personal data.

---

10. Complaints

1.26 Individuals with complaints about the way their personal data has been processed may contact the Clerk or the Information Commissioner's Office at casework@ico.org.uk or call 0303 123 1113.

---

11. Data Transparency

1.37 The Parish Council adheres to the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). This Code helps the Council maintain transparency by publishing public data.

1.39 The principles of the Code are:

1.39.1 **Demand led**: New technologies should support transparency and accountability.
1.39.2 **Open**: Public data will be integral to engagement with residents, driving accountability.
1.39.3 **Timely**: Data will be published promptly after production.

1.41 The Parish Council will publish the following information on its website for public access:

- All transactions above £500
- End-of-year accounts
- Annual Governance Statements
- Internal Audit Reports
- List of Councillors' responsibilities
- Public land and building assets
- Draft minutes of meetings within one month
- Agendas and papers at least three days before meetings

---

12. Making Information Available

1.29 The Parish Council's Publication Scheme encourages public interest and transparency. It specifies what information the Parish Council publishes or intends to publish, with detailed guides available for easy access.

1.33 Formal meetings of the Parish Council are open to the public and press, with reports and relevant background papers available for review. Public participation is welcomed at each meeting.

13. Policy Review

- This policy will be **reviewed at least every two years** to ensure continued compliance with legal requirements and best practices.
- **Adopted by Parish Council:** 20th February 2025
- **Last reviewed:** _____
- **Next review due:** 20th February 2027
- **Signed:** Chairperson: Janet Biggin Parish Clerk: Kevin Spratt

Reference Table for GDPR and SLCC Compliance

Area of Compliance	GDPR Requirement	SLCC Guidance/Best Practice	Policy Section
Transparency and Purpose	GDPR Article 5: Personal data must be processed lawfully, fairly, and transparently.	SLCC recommends transparency in governance and data handling.	Section 1 (Introduction), Section 4 (Protecting Confidential or Sensitive Information)
Lawful Basis for Processing	GDPR Article 6: Personal data processing must have a lawful basis.	SLCC emphasizes compliance with laws and regulations.	Section 5 (When will the Parish Council Process Personal Information?)

Area of Compliance	GDPR Requirement	SLCC Guidance/Best Practice	Policy Section
Consent	GDPR Article 6(1)(a): Consent must be freely given, specific, informed, and unambiguous.	SLCC recommends ensuring clear consent for sensitive data processing.	Section 5 (When will the Parish Council Process Personal Information?)
Sensitive Data	GDPR Article 9: Strict conditions for processing special categories of data.	SLCC advises additional protections for sensitive data.	Section 6 (Sensitive Personal Information)
Data Subject Rights	GDPR Articles 12-23: Individuals' rights include access, correction, deletion, etc.	SLCC encourages councils to ensure data subject rights are respected.	Section 9 (Rights of a Data Subject)
Data Security	GDPR Article 32: Security of processing, ensuring protection from breaches.	SLCC advises on implementing robust data security measures.	Section 8 (Information Security)
Data Retention	GDPR Article 5: Data should not be kept for longer than necessary.	SLCC recommends appropriate retention and deletion protocols.	Section 8 (Information Security), Section 11 (Review History)
Third-Party Processing	GDPR Articles 28-30: Data controllers must ensure third parties are GDPR-compliant.	SLCC advises councils to ensure third-party compliance with data protection laws.	Section 5 (Protecting Confidential or Sensitive Information)
Diversity Monitoring	GDPR Article 9: Specific conditions for processing sensitive personal data (e.g., diversity data).	SLCC recommends data collection for equality monitoring.	Section 10 (Diversity Monitoring)
Data Protection Officer (DPO)	GDPR Articles 37-39: Appointment of a DPO is recommended for large scale processing.	SLCC recommends appointing a DPO for better data governance.	Section 7 (Who is responsible for protecting a person's personal data?)
Public Access and Publication of Data	GDPR Article 15: Access to personal data and transparency in data use.	SLCC encourages making information available to the public and stakeholders.	Section 11 (Making Information Available), Section 12 (Disclosure Information)
Data Transfers Outside EEA	GDPR Article 44: Restrictions on transferring data outside the EEA without adequate safeguards.	SLCC advises on the protection of data in cross-border transactions.	Section 8 (Information Security), Section 13 (Personal data transfer restrictions)