Honeybourne Parish Council

Data Protection Policy

1. Introduction

1.1 The Council holds and processes information about employees, councillors, residents and members of the public, and other data subjects for administrative and public task purposes.

1.2 When handling such information, the Council, and all staff or others who process or use any personal data, must comply with the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The UK GDPR was retained in UK domestic law by the European Union (Withdrawal) Act 2018 and applies in full since the end of the Brexit transition period on 31st December 2020.

1.3 This policy sets out the Council's commitment to lawful, fair and transparent data processing and the responsibilities of all those who handle personal data on the Council's behalf.

2. Data Protection Principles

2.1 There are six principles set out in Article 5 of the UK GDPR. In summary, personal data shall:

- be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- be accurate and, where necessary, kept up to date;
- not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes of processing; and
- be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

2.2 The Council, as Data Controller, is responsible for, and must be able to demonstrate compliance with, these principles (the accountability principle – Article 5(2) UK GDPR).

3. Definitions

3.1 "Employees, councillors, residents and other data subjects" may include past, present and potential members of those groups.

3.2 "Other data subjects" and "third parties" may include contractors, suppliers, contacts, referees, and friends or family members of employees or residents.

3.3 "Processing" refers to any operation or set of operations performed on personal data, including obtaining, recording, storing, adapting, retrieving, using, disclosing, erasing or destroying information.

3.4 "Personal data" means any information relating to an identified or identifiable living individual (a data subject). An identifiable individual is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or one or more factors specific to that person.

3.5 "Special category data" is personal data which, by its nature, is particularly sensitive. UK GDPR Article 9 identifies the following categories: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification); health data; data concerning sex life; and data concerning sexual orientation. Processing special category data requires a specific condition under Article 9(2) UK GDPR in addition to a lawful basis under Article 6.

3.6 "Data Controller" means the person or organisation that determines the purposes and means of processing personal data. The Council is the Data Controller for personal data it holds.

3.7 "Data Processor" means any person or organisation that processes personal data on behalf of the Data Controller, such as contractors or software suppliers used by the Council.

3.8 "Data Protection Lead (DPL)" means the individual appointed by the Council to take operational responsibility for data protection compliance. For this Council the DPL is the Parish Clerk. Note: the Council is not currently required to formally designate a statutory Data Protection Officer under Article 37 UK GDPR, but has appointed a DPL as best practice.

3.9 "Lawful basis" means one of the six conditions in Article 6 UK GDPR which must exist before any personal data is processed. The Council will most commonly rely on: (a) legal obligation; (b) performance of a public task; or (c) legitimate interests, depending on the nature of the processing.

4. Responsibilities

4.1 The Council is the Data Controller and is responsible for ensuring that all processing of personal data for which it is responsible complies with the UK GDPR and the DPA 2018.

4.2 The Data Protection Lead is the Parish Clerk, who acts on behalf of the Council and is responsible for:

- fully observing the conditions regarding the fair collection and use of information;
- meeting the Council's legal obligations to specify the purposes for which information is used;
- ensuring only adequate, relevant and necessary personal data is collected and processed;
- maintaining the quality and accuracy of information;
- ensuring that the rights of data subjects can be fully exercised;
- taking appropriate technical and organisational security measures to safeguard personal information;
- ensuring that personal data is not transferred outside the United Kingdom without suitable safeguards; and
- ensuring that all staff, volunteers and councillors who handle personal data understand their responsibilities, are appropriately trained, and are adequately supervised.

4.3 All councillors and staff must comply with this policy at all times. Appendix A sets out practical guidelines for those who process or may have access to personal data.

4.4 Where the Council engages a third-party Data Processor (for example, payroll providers or software suppliers), a written Data Processing Agreement must be in place in accordance with Article 28 UK GDPR before processing commences. The DPL is responsible for ensuring such agreements are in place and are reviewed periodically.

5. Lawful Basis for Processing

5.1 The Council must identify and document a lawful basis before processing any personal data. Depending on the activity, the Council will rely on one or more of the following:

- **Legal obligation –** where processing is necessary to comply with a legal obligation, for example employer obligations, audit requirements, or statutory council functions.
- **Public task –** where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council.
- **Legitimate interests –** where processing is necessary for the legitimate interests of the Council or a third party, provided those interests are not overridden by the data subject's rights and freedoms.
- **Consent –** where the data subject has given clear, informed and freely given consent. Consent must be recorded and can be withdrawn at any time.

5.2 The Council's lawful bases for its main processing activities are documented in its Record of Processing Activities (ROPA), which is maintained by the DPL and reviewed annually.

5.3 Where the Council processes special category data, an additional condition under Article 9(2) UK GDPR must also be identified and documented.

6. Privacy Notices and Transparency

6.1 The Council has a duty under Articles 13 and 14 of the UK GDPR to provide data subjects with information about how their personal data will be used at the point of collection, or as soon as reasonably practicable where data is not collected directly from the individual.

6.2 The Council meets this duty through its Privacy Notice, which is published on the Council's website and is available from the Parish Clerk on request. The Privacy Notice is reviewed annually and updated whenever there is a material change to processing activities.

6.3 All forms and documents used to collect personal data must include a reference to the Privacy Notice or a brief fair processing statement.

7. Storage and Retention

7.1 Personal data is kept in secure paper-based systems and/or on a password-protected computer system. Access is restricted to those who need it for their work.

7.2 The Council will keep different types of information for different lengths of time, depending on legal, operational and audit requirements. Retention periods are set out in the Council's Retention Schedule, maintained by the Parish Clerk and based on guidance from the National Association of Local Councils (NALC).

7.3 When personal data is no longer required it will be disposed of securely. Paper records containing personal data must be shredded. Electronic records must be permanently deleted.

8. Data Subject Rights

8.1 Under UK GDPR, data subjects have the following rights:

- **The right to be informed –** to receive clear information about how their data is used, met through the Council's Privacy Notice.
- **The right of access –** to obtain a copy of the personal data held about them (Subject Access Request). The Council must respond within one calendar month at no charge.
- **The right to rectification –** to request correction of inaccurate or incomplete personal data.
- **The right to erasure ("right to be forgotten") –** to request deletion of personal data where there is no compelling reason for its continued processing. This right is not absolute and may not apply where processing is required by law.
- **The right to restrict processing –** to request that processing is limited in certain circumstances, for example while accuracy is contested.
- **The right to data portability –** to receive personal data in a structured, commonly used and machine-readable format, where processing is based on consent or contract and carried out by automated means.
- **The right to object –** to object to processing based on public task or legitimate interests. The Council must stop processing unless it can demonstrate compelling legitimate grounds.
- **Rights relating to automated decision-making and profiling –** not to be subject to a decision based solely on automated processing that has a significant effect. The Council does not currently carry out such processing.

8.2 Any data subject wishing to exercise any of the above rights should submit a written request to the Parish Clerk. The Council will respond within one calendar month of receipt. Where requests are complex or numerous, this period may be extended by a further two months; the data subject will be notified within the first month.

8.3 All rights requests must be recorded by the DPL regardless of outcome.

9. Personal Data Breaches

9.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes loss of a device, sending data to the wrong recipient, or accidental deletion.

9.2 Any member of staff, volunteer or councillor who becomes aware of, or suspects, a personal data breach must report it to the Parish Clerk (DPL) immediately.

9.3 Under Article 33 UK GDPR, the Council must notify the Information Commissioner's Office (ICO) of a notifiable breach without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

9.4 Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council must also notify the affected data subjects without undue delay (Article 34 UK GDPR).

9.5 All breaches, whether notifiable or not, must be recorded in the Council's Data Breach Log, maintained by the DPL. The log must include: the date and nature of the breach; the personal data affected; the likely consequences; and the remedial action taken.

10. Data Protection Impact Assessments

10.1 A Data Protection Impact Assessment (DPIA) is required under Article 35 UK GDPR before the Council undertakes any new processing activity that is likely to result in a high risk to the rights and freedoms of individuals. This includes, for example, large-scale processing of special category data or the introduction of new monitoring systems.

10.2 The DPL will determine whether a DPIA is required for any new processing activity and will document the assessment accordingly.

11. Breach of Policy

11.1 Compliance with the UK GDPR and this policy is the responsibility of all councillors and members of staff. Any deliberate or reckless breach of this policy by an employee may lead to disciplinary action and, where appropriate, legal proceedings. Breaches by councillors may result in appropriate action under the Code of Conduct.

11.2 Any individual who believes that the Council has breached any requirement of the UK GDPR or this policy should raise the matter with the Parish Clerk or the Chair of the Council.

11.3 A complaint may also be made directly to the Information Commissioner's Office (ICO): ico.org.uk | 0303 123 1113 | Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

12. Review

This policy will be reviewed every three years, or sooner if there is a change to relevant Legislation or ICO guidance. The DPL is responsible for initiating each review and presenting any amendments to Full Council for approval.

Appendix A – Guidelines for Staff, Volunteers and Councillors

During the course of your duties with the Council, you will handle personal information such as names, addresses, telephone numbers and email addresses of members of the public. You may also encounter sensitive information while carrying out your role.

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 require that personal information is collected and used fairly, stored safely and not disclosed to any other person unlawfully. These guidelines will help you meet those obligations. If you are in any doubt, please contact the Data Protection Lead (Parish Clerk).

Sharing of Personal Information

"Personal information" includes names, addresses, telephone numbers, email addresses, health information and any other details supplied by or about members of the public.

Such information may be shared between staff and councillors of the Council on a strict 'need to know' basis for legitimate work purposes. It must not be disclosed to anyone outside the Council without the explicit consent of the person concerned, or unless there is a clear lawful basis for doing so (for example, a legal obligation). If you are unsure whether you are permitted to share information, please seek advice from the Parish Clerk before doing so.

Unlawful Disclosure of Personal Information

Under the UK GDPR and DPA 2018, you may be committing a criminal offence if you knowingly or recklessly disclose personal information to anyone who is not entitled to receive it. Please take care in any conversations involving personal or sensitive information that could be overheard by those who should not have access to it.

Use of Files, Books and Other Paper Records

To prevent unauthorised access and accidental loss or damage to personal information held on paper, please take good care of files and other paper records and ensure that they are stored securely when not in use. Paper records containing personal data must never be left unattended in public areas.

Use of Email

Before sending emails, check carefully that they do not contain personal or sensitive information that the recipients should not have access to. Take particular care when forwarding emails or adding new recipients to an email chain. You may not forward an email containing another person's personal email address without their prior consent. If in doubt, redact personal email addresses from the body of any email chain before forwarding.

Use of Devices and Electronic Systems

The Council does not provide devices to councillors. Where councillors or staff access Council data or email on personal devices, they must ensure those devices are password or PIN protected, that Council emails and documents are not forwarded to personal email accounts, and that any Council data held on a personal device is deleted securely when it is no longer needed. Portable devices such as USB drives containing personal data must be encrypted where possible.

Disposal of Documents

Any paper documents containing personal or sensitive information must be destroyed securely by shredding. For larger quantities of confidential waste, the Council may arrange secure

collection with a certificated contractor. Personal data must never be placed in general waste or recycling.

Reporting a Data Breach

If you become aware of, or suspect, a personal data breach – including accidental loss or disclosure, sending data to the wrong recipient, or loss of a device – you must report it to the Parish Clerk immediately. Do not attempt to deal with the breach yourself without first notifying the Parish Clerk. Prompt reporting is essential; the Council may have a legal obligation to notify the ICO within 72 hours.