HEADBOURNE WORTHY

PARISH COUNCIL

Data Protection Policy

Adopted by Headbourne Worthy PC

January 2025

CONTENTS

CLAUSE

1 INTRODUCTION

1.1 This Data Protection Policy sets out how Headbourne Worthy Parish Council ("we", "our", "us", "the Council") handle the Personal Data of our parishioners, councillors, suppliers, employees, workers, business contacts and other third parties.

1.2 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.

1.3 This Data Protection Policy applies to all Councillors and Council Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf. Data protection is the responsibility of everyone within the Council and this Data Protection Policy sets out what we expect from you when handling Personal Data to enable the Council to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action.

1.4 This Data Protection Policy is an internal document and cannot be shared with third parties without prior authorisation from the DPO.

2 INTERPRETATION

2.1 In this policy certain terms are used which have the following meanings:

Council Personnel	all employees, workers, contractors, agency workers, consultants, and others.
Consent	agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.
Controller	the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our Council Personnel and the functioning of the Council.
Criminal Convictions Data	personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.
Data Subject	a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or

	residents of any country and may have legal rights regarding their Personal Data.
Data Protection Officer (DPO)	either of the following: (a) the person required to be appointed in specific circumstances under the UK GDPR; or (b) where a mandatory DPO has not been appointed, a data privacy manager or other voluntary appointment of a DPO with responsibility for data protection compliance.
Explicit Consent	consent which requires a very clear and specific statement (that is, not just action).
UK GDPR	the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.
Personal Data	any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data Breach	any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies	separate notices setting out information that may be provided to Data Subjects when the Council collects information about them. These notices may take the form of: (a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or

	(b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.
Processing or Process	any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Pseudonymisation or Pseudonymised	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.
Special Categories of Personal Data	information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

3 SCOPE OF POLICY AND WHEN TO SEEK ADVICE ON DATA PROTECTION COMPLIANCE

3.1 Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Council is exposed to potential fines for failure to comply with the UK GDPR.

3.2 All Councillors and Council Personnel are responsible for ensuring compliance with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3.3 The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies. That post is held by [NAME], and they can be reached at [TELEPHONE NUMBER] and [EMAIL ADDRESS].

3.4 Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

3.4.1 if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by the Council) (see paragraph 5.1);

3.4.2 if you need to rely on Consent or need to capture Explicit Consent (see paragraph 6);

3.4.3 if you need to draft Privacy Notices (see paragraph 7);

3.4.4 if you are unsure about the retention period for the Personal Data being Processed (see paragraph 11);

3.4.5 if you are unsure what security or other measures you need to implement to protect Personal Data (see paragraph 12.1);

3.4.6 if there has been a Personal Data Breach (paragraph 13);

3.4.7 if you are unsure on what basis to transfer Personal Data outside the UK (see paragraph 14);

3.4.8 if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 15);

3.4.9 whenever you plan to use Personal Data for purposes other than for which it was collected (see paragraph 8); or

3.4.10 if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (see paragraph 18).

4 PERSONAL DATA PROTECTION PRINCIPLES

4.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

4.1.1 Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

4.1.2 collected only for specified, explicit and legitimate purposes (purpose limitation);

4.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

4.1.4 accurate and where necessary kept up to date (accuracy);

4.1.5 not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

4.1.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

4.1.7 not transferred to another country without appropriate safeguards in place (transfer limitation); and

4.1.8 made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

5 LAWFULNESS, FAIRNESS AND TRANSPARENCY

5.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 We may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

5.3.1 the Data Subject has given their Consent;

5.3.2 the Processing is necessary for the performance of a contract with the Data Subject;

5.3.3 to meet our legal compliance obligations;

5.3.4 to protect the Data Subject's vital interests;

5.3.5 to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

5.4 The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices, or we must identify and document the legal ground being relied on for each Processing activity.

6 CONSENT

6.1 A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

6.2 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.3 A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.4 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

6.5 We will need to evidence Consent captured and keep records of all Consents so that the Council can demonstrate compliance with Consent requirements.

7 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

7.1 The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

7.2 Whenever we collect Personal Data directly from a Data Subject we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

7.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

8 PURPOSE LIMITATION

8.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

8.2 We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and they have Consented where necessary.

8.3 If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the DPO for advice on how to do this in compliance with both the law and this Data Protection Policy.

9 DATA MINIMISATION

9.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

9.2 You may only Process Personal Data when performing your duties requires it. You cannot Process Personal Data for any reason unrelated to your duties.

9.3 You may only collect Personal Data that you require for your duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

9.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised.

10 ACCURACY

10.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

10.2 We must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it.

11 STORAGE LIMITATION

11.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed including for the purpose of satisfying any legal, accounting or reporting requirements

11.2 We will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

12 SECURITY INTEGRITY AND CONFIDENTIALITY

12.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

12.2 We will develop, implement and maintain safeguards appropriate to our role as a Parish Council, our available resources, the amount of Personal Data that we own or maintain, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate those safeguards to ensure security of our Processing of Personal Data.

12.3 You are also responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data when in your possession. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

12.4 You must follow all procedures we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

12.5 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

12.5.1 Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

12.5.2 Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

12.5.3 Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

13 REPORTING A PERSONAL DATA BREACH

13.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

13.2 We will notify the Data Subject or any applicable regulator where we are legally required to do so.

13.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

14 TRANSFER LIMITATION

14.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

14.2 We will only transfer Personal Data outside the UK if one of the following conditions applies:

14.2.1 the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

14.2.2 appropriate safeguards are in place such as binding corporate rules, or standard contractual clauses approved for use in the UK;

14.2.3 the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

14.2.4 the transfer is necessary for one of the other reasons set out in the UK GDPR including:

(a) the performance of a contract between us and the Data Subject;

(b) reasons of public interest;

(c) to establish, exercise or defend legal claims;

(d) to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and

(e) in some limited cases, for our legitimate interest.

15 DATA SUBJECT'S RIGHTS AND REQUESTS

15.1 A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:

15.1.1 withdraw Consent to Processing at any time;

15.1.2 receive certain information about the Controller's Processing activities;

15.1.3 request access to their Personal Data that we hold (including receiving a copy of their Personal Data);

15.1.4 prevent our use of their Personal Data for direct marketing purposes;

15.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

15.1.6 restrict Processing in specific circumstances;

15.1.7 object to Processing which has been justified on the basis of our legitimate interests or in the public interest;

15.1.8 request a copy of an agreement under which Personal Data is transferred outside of the UK;

15.1.9 object to decisions based solely on automated processing, including profiling (ADM);

15.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

15.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

15.1.12 make a complaint to the supervisory authority; and

15.1.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

15.2 You must immediately forward any Data Subject request you receive to the DPO.

15.3 The DPO will verify the identity of an individual requesting data under any of the rights listed above.

15.4 Do not allow third parties to persuade you into disclosing Personal Data without proper authorisation.

16 ACCOUNTABILITY

16.1 As a Controller we must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2 The Council must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

16.2.1 appointing a DPO accountable for data privacy;

16.2.2 implementing appropriate technical and organisational measures to ensure that Personal Data is kept secure when Processing it;

16.2.3 integrating data protection into internal documents including this Data Protection Policy, related policies or Privacy Notices;

16.2.4 regularly assessing compliance.

17 RECORD KEEPING

17.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities including records of Data Subjects' Consents and procedures for obtaining Consents.

17.2 These records should include, at a minimum:

17.2.1 the name and contact details of the Controller and the DPO; and

17.2.2 clear descriptions of:

(a) the Personal Data types;

(b) the Data Subject types;

(c) the Processing activities;

(d) the Processing purposes;

(e) the third-party recipients of the Personal Data;

(f) the Personal Data storage locations;

(g) the Personal Data transfers;

(h) the Personal Data's retention period; and

(i) the security measures in place.

18 SHARING PERSONAL DATA

18.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

18.2 You may only share the Personal Data we hold with another Councillor, employee, agent or representative of our Council if the recipient has a role-related need to know the information.

18.3 You may only share the Personal Data we hold with third parties, such as our service providers, if:

18.3.1 they have a need to know the information for the purposes of providing the contracted services;

18.3.2 sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

18.3.3 the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;

18.3.4 the transfer complies with any applicable cross-border transfer restrictions; and

18.3.5 a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

19 CHANGES TO THIS DATA PROTECTION POLICY

19.1 We keep this Data Protection Policy under regular review. This version was last updated on January 2025.