West Horsley Parish Council

DATA PROTECTION POLICY

1. Introduction

West Horsley Parish Council (WHPC) has a responsibility as a data controller under the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR) and the Data (Use and Access) Act 2025 to hold, obtain, record, use and store all personal data relating to an identifiable individual in a secure and confidential manner. This policy is a statement of what WHPC does to ensure its compliance with the DPA.

The policy applies to all WHPC employees, councillors and contractors. It provides a framework within which the Parish Council will ensure compliance with the requirements of the DPA and will underpin any operational procedures and activities connected with the implementation of the legislation.

As well as this overarching policy, data protection principles are also embedded within many of the Council's other policies and procedures.

WHPC will use all appropriate and necessary means at its disposal to comply with the DPA and associated guidance.

2. Background

The DPA governs the handling of personal information that identifies living individuals directly or indirectly and covers both manual and computerised information. It provides a mechanism by which individuals about whom data is held (the 'Data Subjects') can have a certain amount of control over the way in which it is handled.

Some of the main features of the DPA are:

- All data covered by the DPA must be handled in accordance with Seven Data Protection Principles (see Appendix 1).
- The Data Subject has various rights under the DPA. Refer to the council's **Subject Access Request Policy** for further information.
- UK GDPR and the Data Protection Act 2018 are currently the main data protection laws in the UK. The Data (Use and Access) Act 2025 is a recent update changing aspects of those laws and will shape how data protection works going forward. All relevant legislation will be referred to as 'DPA' throughout this document.
- Processing of special categories of data must be done under a lawful basis. This data includes information about race, ethnic origin, political persuasion, religious belief, trade union membership, genetics, biometrics (where used for identification purposes), health, sex life and sexual orientation.
- The DPA deals with criminal offence data in a similar way to special category data and sets out specific conditions providing lawful authority for processing it.
- Data controllers are accountable for protecting personal data by putting suitable technical and organisational measures in place. This includes having internal data protection policies and procedures, training staff on DPA requirements, keeping records of processing activities, and

applying data protection by design and by default—such as minimising data, ensuring transparency, and continuously improving security measures.
- Data protection impact assessments are carried out where appropriate as part of the design and planning of projects, systems and programmes.
- Data controllers must have written contracts in place with all data processors and ensure that processors are only appointed if they can provide 'sufficient guarantees' that the requirements of the DPA will be met and the rights of Data Subjects protected. A list of these data processors can be seen in the council's **Data Audit**.
- Data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office within 72 hours of the council becoming aware of the breach. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the council will notify those individuals concerned directly (see the Council's '**Data Breach Policy**' for further information).
- The Information Commissioner is responsible for regulation and issues notices to organisations if they are not complying with the requirements of the DPA. They can also prosecute those who commit offences under the legislation and issue fines.

3. Roles and Responsibilities

Section 7(3) of the DPA 2018 states that town and parish councils are not recognised as public bodies for GDPR purposes and so are not required to appoint a Data Protection Officer. However, the Parish Council is still subject to data protection legislation and must ensure that the council has sufficient staff and resources to discharge its obligations under the DPA.

The Parish Clerk is responsible for the following tasks:

- Informing and advising the Parish Council, any processor engaged by the Parish Council as data controller, and any employee of the Parish Council who carries out processing of personal data, of that person's obligations under the legislation
- Ensuring Parish Council policies continue to comply with the legislation
- Co-operating with the Information Commissioner's Office (ICO),
- Advising and monitoring on data protection impact assessments

As the data controller, the Parish Council must provide the clerk with the necessary resources and access to personal data and processing operations to enable them to perform the tasks outlined above and to maintain their expert knowledge of data protection law and practice.

The Parish Council will be responsible for ensuring that it complies with its responsibilities under the DPA through monitoring of activities and incidents. The Parish Council will also ensure that there are adequate resources to support the work outlined in this policy to ensure compliance with the DPA.

All staff and councillors will ensure that:

- Personal information is treated in a confidential manner in accordance with this and any associated policies
- The rights of Data Subjects are respected at all times, and privacy notices are available to inform individuals how their data is being processed
- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose

- Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information
- Personal information held within applications, systems, personal or shared drives is only accessed to carry out work responsibilities
- Personal information is recorded accurately and is kept up to date
- They refer any subject access requests and/or requests in relation to the rights of individuals to the clerk
- They raise actual or potential breaches of the DPA to the clerk as soon as the breach is discovered
- It is the responsibility of all staff and councillors to ensure that they comply with the requirements of this policy and any associated policies or procedures.

Where contractors are used, the contracts between the Parish Council and these third parties should contain mandatory information assurance clauses to ensure that the contract staff are bound by the same code of behaviour as parish council members of staff and councillors in relation to the DPA.

4. Records Management

Good records management practice plays a pivotal role in ensuring that the parish council can meet its obligations to provide information, and to retain it, in a timely and effective manner to meet the requirements of the DPA. All records should be retained and disposed of in accordance with the council's '**Retention and Disposal Policy'**.

5. Consent

The Parish Council will take all reasonable steps to ensure that service users, members of staff and contractors are informed of the reasons the Parish Council requires information from them, how that information will be used and who it will be shared with. This will enable the Data Subject to give explicit informed consent to the Parish Council handling their data where the legal basis for processing is consent.

Should the Parish Council wish to use personal data for any purpose other than that specified when it was originally obtained, the Data Subject's explicit consent should be obtained prior to using the data in the new way unless exceptionally such use is in accordance with other provisions of the DPA.

Should the Parish Council wish to share personal data with anyone other than those recipients specified at the time the data was originally obtained, the Data Subject's explicit consent should be obtained prior to sharing that data, failure to do so could result in a breach of confidentiality.

6. Accuracy and Data Quality

The Parish Council will ensure that all reasonable steps are taken to confirm the validity of personal information directly with the Data Subject.

All members of staff and councillors must ensure that service user personal information is checked and kept accurate and up to date on a regular basis, for example, by checking it with the service user when they attend for appointments in order that the information held can be validated.

Where a member of the public exercises their right for their data to be erased, rectified, or restricted, or where a member of the public objects to the processing of their data, the clerk must be notified and the appropriate procedures followed.

7. Data Protection Impact Assessments

A data protection impact assessment is a process which helps to assess privacy risks to individuals in the collection, use and disclosure of information. Where applicable and as advised by the clerk, they must be carried out at the early stages of projects.

8. Providers

The Parish Council must have written contracts in place with all suppliers who process personal data on behalf of the parish council as "data processors". The Parish Council will ensure that processors are only appointed if they can provide 'sufficient guarantees' through the procurement process that the requirements of the DPA will be met and the rights of Data Subjects protected.

9. Complaints

Any expression of dissatisfaction with reference to the Parish Council's handling of personal information will be treated as a complaint and handled under WHPC's **Complaints Procedure**.

Should the complainant remain dissatisfied with the outcome of their complaint to the Council, a complaint can be made to the Information Commissioner's Office who will then investigate the complaint and act where necessary.

10. Security and Confidentiality

All staff and councillors must ensure that information relating to identifiable individuals is always kept secure and confidential. The Parish Council will ensure that its holdings of personal data are properly secured from loss or corruption and that no unauthorised disclosures of personal data are made.

WHPC will ensure that information is not transferred to countries outside the European Economic Area (EEA) unless that country has an adequate level of protection for security and confidentiality of information which has been confirmed by the ICO.

11. Rights of Data Subjects

Individuals wishing to request their information as a subject access request should contact the Parish Council, who will arrange for the information to be processed in accordance with the DPA. Further information on this is available in a separate **Subject Access Request Policy**.

Individuals should also make requests in writing to the Parish Council if they wish to exercise their other rights under the legislation.

For review and approval by Full Council on 21 July 2026

Next review: July 2028

APPENDIX 1 DATA PROTECTION PRINCIPLES

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

7. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').