Hedgerley Parish Council Data Protection Policy

1. POLICY STATEMENT

During the course of the Parish Council's activities, it will collect, store and process personal information about its staff and Councillors, and it recognises the need to treat all Data in an appropriate and lawful manner.

The types of information that the Parish Council may be required to handle include details of current, past and prospective employees, and suppliers. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (DPA 2018) and other regulations. The DPA 2018 stipulates how it may use that information. The Parish Council has ultimate responsibility for ensuring compliance with Data Protection legislation.

2. STATUS OF THE POLICY

This policy sets out the Parish Council's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information. If you consider that the policy has not been followed in respect of personal data about yourself or others, you should raise the matter with the Clerk to the Parish Council.

3. DEFINITION OF DATA PROTECTION TERMS

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data is data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controller is the Proper Officer of the Parish Council, who determines the purposes for which, and the manner in which any personal data is processed. They have a responsibility to establish practices and policies in line with DPA 2018.

Data user will be the Proper Officer of the Parish Council whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the 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 transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

• Processed fairly and lawfully.

• Processed for limited purposes and in an appropriate way.

• Adequate, relevant and not excessive for the purpose.

• Accurate.

• Not kept longer than necessary for the purpose.

• Processed in line with data subjects' rights.

• Secure.

• Not transferred to people or organisations situated in countries without adequate protection.

5. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from the Parish Council's systems when it is no longer required. All records should be retained and disposed of in accordance with ICO guidance.

6. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. The Parish Council must ensure individuals can exercise their rights in the following ways:

• Right to be informed: providing privacy notices o keeping a record of how the Parish Council uses personal data to demonstrate compliance

• Right of access: enabling individuals to access their personal data and supplementary information be aware of and verifying the lawfulness of the processing activities

• Right to rectification: rectifying or amending personal data of the individual if requested and carrying out the process within one month

• Right to erasure: deleting or removing an individual's data if requested and there is no compelling reason for its continued processing.

• Right to restrict processing: complying with any request to restrict, block or supress the processing of personal data retaining only enough data to ensure the right to restriction is respected in the future

• Right to data portability: providing individuals with their data so that they can reuse it for their own purposes and providing it in a commonly used format (i.e. machine-readable format)

• Right to withdraw consent: respecting the right of an individual to withdraw consent to the processing at any time for any processing of data to which consent was obtained withdrawal can be by telephone, email or by post.

• The right to lodge a complaint with the Information Commissioner's Office.

Information Commissioners Office
Phone: 0303 123 1113
Email: https://ico.org.uk/global/contact-us/email/
Post: Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow,
Cheshire SK9 5AF.

7. DATA SECURITY

The Parish Council will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of/damage to personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss. DPA 2018 requires procedures and technologies to be put in place to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with the procedures and policies, or if they put in place adequate measures. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

a) Confidentiality means that only the Proper Officer is authorised to use the data and can access it.

b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

c) Availability means that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures include:

• Secure lockable drawers and/or cupboards. Drawers and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

• All computers used to access or process Parish Council personal data must have virus protection and a firewall.

• Password protection is used.

• Methods of disposal. Paper documents should be shredded. Electronic data will be deleted.

8. RECORDS MANAGEMENT AND DATA AUDIT

Good records management are essential in ensuring that the Parish Council is able to meet its obligations to provide information and to retain it in a timely and effective manner in order to meet the requirements of DPA 2018. All records should be retained and disposed of in accordance with ICO guidance.

9. DATA PROTECTION IMPACT ASSESSMENTS

Data Protection Impact Assessments Data protection impact assessments will be carried out where appropriate.

10. DATA BREACHES

Under GDPR the Parish Council is required to report a personal data breach which meets the reporting criteria to the Information Commissioner within 72 hours of the Council becoming aware of the breach. Guidance states that organisations should notify the ICO of a breach where it is likely to result in:

- a risk to the rights and freedoms of individuals
- if it could result in discrimination
- damage to reputation
- financial loss
- loss of confidentiality
- or any other significant economic or social disadvantage.

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

In the event of a data breach the Proper Officer will immediately inform the Chair of the Parish Council. They will then take all the necessary measures to manage the breach. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Parish Council will notify those individuals concerned directly. In line with the accountability requirements, all data breaches must be recorded by the Parish Council along with details of actions taken. This record will help to identify system failures and should be used to improve the security of personal data.

11. DEALING WITH SUBJECT ACCESS REQUESTS (SAR)

The Parish Council is aware that people have the right to access any personal information that is held about them. If a person requests to see any data that is being held about them, this will be handled in accordance with the ICO Guidance to Subject Access Requests.

12. ACCESS TO POLICIES REFERRED TO UNDER THIS POLICY

For details of all of the polices relevant to Hedgerley Parish Council as a local government authority please visit the Parish Council's website: www.hedgerleyparishcouncil.gov.uk