HOOE PARISH COUNCIL

HOOE PARISH COUNCIL

DATA PROTECTION POLICY

Policy adopted on 7th December 2022 – Agenda Item 10d

1. The Data Protection Policy

Hooe parish council will comply with the General Data Protection Regulations 2018 in carrying out its functions as a local council. Other legislation that is also relevant includes the Freedom of Information Act 2000, The Computer Misuse Act 1990, The Crime and Disorder Act 1998 and the Human Rights Act 1998.

The General Data Protection Regulations 2018 sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. This includes employees, councillors, volunteers, residents and service users and other data subjects for administrative and commercial purposes.

This policy applies to the collection and processing of all personal data held by the parish council, falling within the scope of the General Data Protection Regulations 2018 and the Data Protection Act 2018 in all formats including paper, electronic, audio and visual.

2. Roles and Responsibilities

Hooe parish council is the **Data Controller** and must ensure that any processing of personal data for which the parish council is responsible, complies with the General Data Act 2018.

The Clerk

The clerk has the overall responsibility for ensuring that the parish council complies with all relevant data protection obligations and acts as the representative of the data controller on a day to day basis.

Data Protection Officer

The parish council is not required to employ a Data Protection Officer (DPO), and the clerk is responsible for overseeing and implementation of this policy, monitoring the compliance with data protection law, and developing related policies and guideline where applicable.

3. Data Protection Principles

When processing personal data, the following principles must be applied to demonstrate good practice and includes:

Data is processed fairly, lawfully and in a transparent manner

This means that personal information should be processed lawfully, fairly and in a transparent manner in relation to individuals.

Data is processed for specified purposes only

This means that data is collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes.

Data is relevant to what it is needed for

Data will be monitored so that too much or too little is not kept; only data that is needed should be held.

Data is accurate and kept up to date and is not kept longer than it is needed

Personal data should be accurate, where necessary kept up to date, ensuring steps are taken to confirm the data is accurate and only kept for the purposes which it is to be used, and erased when appropriate to do so.

Data is processed in accordance with the rights of individuals

Individuals must be informed, upon request, of all the personal information held about them.

Data is kept securely

Data should be 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.

4. Data Protection Officer Responsibilities

The **Data Protection Officer** is the clerk, who acts on behalf of the council, and is responsible for:

- Fully observing conditions regarding the fair collection and use of information
- Meeting the Council's legal obligations to specify the purposes for which information is used
- Collecting and processing relevant information, only to the extent that is required to fulfil operational needs/to comply with legal requirements
- Ensuring the quality of information used
- Applying strict checks to determine the length of time that information is held
- Ensuring that the rights of the people whom the information is held can be fully exercised under the Data Protection Act
- Taking appropriate technical and organisational security measures to safeguard personal information
- Ensuring that personal information is not transferred abroad without suitable safeguards
- Ensuring that everyone managing and handling personal information fully understands that they are contractually responsible for following good practice in terms of protection and is adequately trained to do so.

5. Storage and Retention

Personal data are kept in paper based systems, securely kept and / or on a password protected computer system.

The parish council will keep different types of information for different lengths of time, depending on legal and operational requirements. More information can be found in the parish council's **Documentation Retention Policy**.

6. Access to Information

Any employee, councillor, resident, volunteer, service user and other data subjects have rights to access any personal information that is held about them by submitting a **Subject Access Request** which may include:

- To ask what personal information the parish council holds
- To ask what this information is used for
- To be provided with a copy of the information
- To be given details of the purpose for which the parish council uses the information and any other persons, organisations to whom it is disclosed
- To ask that any incorrect data held is corrected

Subject Access Requests (SARs) must be submitted in writing. If a person requests to see any data that is being held about them. The parish council should respond within 20 working days and is free of charge.

If the SAR includes personal data of other individuals, Hooe parish council must not disclose the personal information of the other individual. That individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the subject.

Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restrictions of processing of the data and the right to object to data processing, although **rules** do apply to these requests.

7. Data Security

The General Data Protection Regulations and the Data Protection Act requires that appropriate technical and organisational measures shall be put in place to protect the data against:

- Unauthorised access
- Unauthorised or unlawful processing
- Accidental loss, destruction or damage

Appropriate technical and organisational security measures will include:

- Using and developing technological solutions to ensure compliance with the data protection principles
- Using and developing physical measures to protect the parish council assets
- Ensuring the reliability of any persons who have access to parish council information
- Reporting and investigating security breaches

These obligations include the need to consider the nature of the data to be protected and the harm that might arise from such unauthorised or unlawful processing or accidental loss, destruction or damage.

All printout material, magnetic tape, diskettes, CD'S OR DVD'S, manual files, handwritten notes etc., which contain personal data and are no longer required, will be treated as confidential waste, and disposed of securely.

8. Personal Data Breaches

The parish council will make all reasonable endeavors to ensure that there are no personal data breaches.

Where appropriate, the parish council will report a data breach to the Information Commissioner's Office within 72 hours. Such breaches in a parish council context may include, but are not limited to:

- The theft of a parish council personal electronic device containing non-encrypted personal data about members / employees and / or residents etc.
- Accidental disclosure of personal data to another person or organisation
- Inappropriate access to or use of personal data
- The theft of personal information, either paper based or electronic
- Accidental loss of personal data
- Information that has not arrived at its destination
- Fraudulent acquisition of personal information (Blaggers)

As well as the parish council, any individual who knowingly or recklessly processes data without appropriate consent or proper authorisation, for the purposes other than those for which it is intended or is deliberately acting outside their recognised responsibilities may be subject to the parish council's disciplinary procedures if an employee, or as **an individual may be subject to legal action and prosecution and possible criminal conviction under the Criminal Justice and Immigration Act 2008.**