DATA PROTECTION POLICY[1]

Introduction
St Dennis Parish Council has a responsibility under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 to hold, obtain, record, use and store all personal data relating to an identifiable individual in a secure and confidential manner. This Policy sets out the Parish Councils approach to data protection and the responsibilities of those who handle personal data on the Councils behalf whilst ensuring compliance with the legislation.

This Data Protection Policy applies to all Parish Council employees, Councillors, volunteers, and contractors who process personal data on behalf of the Council. The Policy provides a framework within which the Parish Council will ensure compliance with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and will underpin any operational procedures and activities connected with the implementation.

St Dennis Parish Council is registered with the Information Commissioner's Office (ICO) under Register Entry No. ZA089226

This policy is complemented by the Council's Privacy Notice, which provides more detailed information about how personal data is collected, used, and protected. The Privacy Notice is available on the Parish Council website or from the Parish Council Office on request.

Background
The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 govern 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. Where the Council processes personal data relating to children, it will do so only where it has a lawful basis and appropriate safeguards are in place. The Council will only process personal data where it has a lawful basis under Article 6 UK GDPR, and special category data only where an Article 9 condition also applies.

Some of the key features of the legislation are:

- All data covered by the legislation must be handled in accordance with the Seven Data Protection Principles. They are as follows –
    - First Principle "processed lawfully, fairly and in a transparent manner in relation to individuals."
    - Second Principle "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purp".es in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes";
    - Third Principle "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."
    - Fourth Principle "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate,

[1] Adopted by Full Council on the meeting held on 04th August 2026 under minute number 160/26. Due for review in 2027 or before if a change in legislation.

having regard to the purposes for which they are processed, are erased or rectified without delay."

- Fifth Principle "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"; and
- Sixth Principle "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."
- Seventh Principle "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 organised measures (integrity and confidentiality)."

- The person about whom the information is held (the "data subject") has various rights under the Act, including the right to be informed about what personal data is being processed, the right to request access to that information, the right to request that inaccuracies, or incomplete data, are rectified, and the right to have personal data erased and to prevent, or restrict, processing in specific circumstances. Individuals also have the right to object to processing based on the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling); and processing for the purposes of scientific/historical research and statistics. There are also rights concerning automated decision making (including profiling) and data portability.

- 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 Data Protection Act 2018 deals with criminal offence data in a similar way to special category data and sets out specific conditions providing lawful authority for processing it.

- There is a principle of accountability of data controllers to implement appropriate technical and organisational measures that include internal data protection policies and procedures, staff training and awareness of the requirements of the Act, internal audits of processing activities, maintaining relevant documentation on processing activities, appointing a data protection officer, and implementing measures that meet the principles of data protection by design and data protection by default, including data minimisation, transparency, and creating and improving security features on an ongoing basis.

- 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 Act will be met and the rights of data subjects protected.

- A data breach is defined as a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.' 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 Controller 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.

- The Information Commissioner is responsible for regulation and issue notices to organisations where they are not complying with the requirements of the Act. The Information Commissioner also has the ability to prosecute those who commit offences under the Act, and to issue fines.

<u>Roles and Responsibilities</u>
Data Protection Officer
The Data Protection Officer is the Clerk who is responsible for the following tasks -

- Informing and advising the Parish Council, as data controller, and any employee of the Council who conducts processing of personal data, of that person's obligations under the legislation.
- Providing advice and monitoring for the conducting of a data protection impact assessments.
- Take any reasonable necessary steps to ensure the security of council data; this shall include to ensure that access to data is limited and that data is disposed of securely. and
- Co-operating with the Information Commissioner's Office and acting as the contact point for the Information Commissioner's Office.

The Parish Council is committed to providing the Data Protection Officer 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.

Data Controller – St Dennis Parish Council
St Dennis Parish Council is the data controller.

The Parish Council will be responsible for ensuring that the organisation complies with its responsibilities under the Data Protection Act 2018 through monitoring of activities and incidents via reporting by the Data Protection Officer.

All Staff and Councillors
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.

- Privacy notices will be made 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 in order 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 Data Protection Officer.

- They raise actual or potential breaches of the Data Protection Act to the Data Protection Officer 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. All must undertake mandatory annual data protection training.

Contractors
Where the Council appoints contractors or suppliers to process personal data on its behalf, written contracts must include appropriate data protection and confidentiality clauses and require the processor to act only on the Council's instructions.
Volunteers
Volunteers who handle personal data on behalf of the Council must follow this policy and any associated procedures in the same way as staff and Councillors.

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 in order to meet the requirements of the Act. All records should be retained and disposed of in accordance with the Retention of Documents policy, which is available on the Parish Council website or on request from the Parish Council Office.

Consent
Where the Council relies on consent as the lawful basis for processing personal data, it will ensure that consent is freely given, specific, informed and unambiguous. If the Council wishes to use personal data for a new purpose, it will check whether that purpose is compatible with the original purpose and, where necessary, obtain a new lawful basis or fresh consent.

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 Data Protection Officer must be notified and the appropriate procedures followed.

Data Protection Impact Assessments (DPIA's)
A data protection impact assessment (DPIA) is a process which helps to assess privacy risks to individuals in the collection, use and disclosure of information. They must be carried out at the initial stages of projects and are embedded into the Parish Council's decision-making process. DPIAs will be completed where processing is likely to result in a high risk to the rights and freedoms of individuals, in accordance with Article 35 of the UK GDPR.

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 Act will be met and the rights of data subjects protected.

Complaints
Any complaint about the Council's handling of personal data will be handled in accordance with the Council's complaints procedure.

The Data Protection Officer (DPO) will log and monitor data-related complaints to identify trends or recurring issues. This ensures that the Council can take proactive measures to improve its data protection practices and address any concerns.

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 take action where necessary.

Security and Confidentiality
All staff and Councillors must ensure that information relating to identifiable individuals is kept secure and confidential at all times. 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.

The Council uses appropriate technical (e.g., encryption, secure servers) and organisational measures (e.g., policies, access controls) to protect data, ensuring that personal information is safeguarded against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

The Parish Council will ensure that information is not transferred to countries outside the United Kingdom unless those countries are covered by UK adequacy regulations or appropriate safeguards are in place (e.g., standard contractual clauses) in accordance with UK GDPR requirements. Please note that the Parish Council website and social media accounts are

accessible from overseas, so on occasion some personal data (for example, in a newsletter) may be accessed from abroad.

Rights of Data Subjects
A data subject has the right to:

a. a. access their personal data;
b. request rectification of inaccurate or incomplete data;
c. request erasure;
d. object to processing in certain circumstances;
e. request restriction of processing;
f. request data portability where applicable;
g. withdraw consent where consent is the lawful basis; and
h. complain to the Information Commissioner's Office.
Individuals wishing to request their information as a subject access request should refer to the Subject Access Requests Policy.

Review
This policy will be reviewed every three years or sooner if legislative changes require.