St Enoder Parish Council

Data Protection Policy.

1. Introduction

The policy has been revised due to the introduction of General Data Protection Regulation which comes into force on 25th May 2018. The previous policy was produced in line with the previous piece of legislation (Data Protection Act 1998). Much of the general content remains the same in that personal data should be handled with care and integrity and not be used for purposes other than it was intended for. The General Data Protection Regulation (GDPR) established a framework of rights and duties which safeguard personal data. Personal data is information about a living individual who can be identified from the data (including photographs). This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

St Enoder Parish Council is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with GDPR. The Council has established the following policy to support this commitment. It is the personal responsibility of all employees, Members, contractors, agents and anyone else processing information on behalf of the Parish Council to comply with this policy. This policy continues to apply to employees and individuals even after their relationship with the Council ends.

The Parish Council is regarded as the Data Controller and is responsible for the legal processing and handling of data. Compliance with the GDPR will be monitored by the Information Commissioner's Office (ICO). The Parish Council is already registered with the ICO as a Data Controller. Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation. GDPR breaches could lead to significant fines. All potential breaches will be investigated and action may be taken by the Council's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and/or criminal action being taken.

2. **Data Protection Principles**

GDPR is underpinned by a set of six common-sense principles, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using and holding, disclosing and deleting personal data.

Personal data must be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

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 appropriated technical or organisational measures.

3. Access and Use of Personal Data

Access and use of personal data held by the Council is only permitted by employees, Members, contractors, agents and anyone else processing information on behalf of the Parish Council for the purpose of carrying out their official duties. Use for any other purpose is prohibited.
Deliberate unauthorised access to, copying, disclosure, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal offence and/or disciplinary offence.
It is an offence under GDPR any person to knowingly or recklessly obtain, procure or disclose personal data without the permission of the data controller (St Enoder Parish Council) subject to certain exception.

4. Collecting Personal Data

When personal data is collected, for example on a questionnaire, survey or form, the data subject (that is to say the person who the information is about) must be told, unless this is obvious to them, which organisation(s) they are giving their information to; what their information will be used for; who it may be shared with and anything else that might be relevant e.g. the consequences of that use. This is known as a Privacy Notice.
Personal data collected must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where de-personalised (anonymous) information would suffice. If the information is collected for one purpose, it cannot subsequently be used for a different and unconnected purpose without the data subject's consent (unless there is another lawful basis for using the information - see section 5 below). It must be made clear to the data subject at the time the information is collected what other purposes their information may be used for.

5. Lawful Basis for Processing

When St Enoder Parish Council processes personal data, it must have a lawful basis for doing so. GDPR provides a list of "conditions" when personal or sensitive personal data may be processed. GDPR defines "sensitive" personal data as information relating to a person's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health condition; sexual life; criminal offences (alleged or committed). The Parish Council can also process personal data if it has the data subject's consent (this needs to be explicit when it processes sensitive personal data). In order for consent to be valid it must be "fully informed" which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress.

6. Disclosing Personal Data

Personal data must not be disclosed to anyone internally or externally unless the person disclosing the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information. If personal data is disclosed to another organisation or person outside of the Parish Council, the disclosing person must identify their lawful basis for the disclosure and record their decision. This should include a description of the information disclosed; the name of the person and organisation to which the information was disclosed; the date; the reason for the

disclosure; the lawful basis.
In response to any lawful request, only the minimum amount of personal information should be disclosed. The person disclosing the information should ensure that the information is adequate for the purpose of the disclosure, relevant and not excessive.

7. Accuracy and Relevance

It is the responsibility of those who receive personal information to ensure so far as possible that it is accurate and up to date. Personal information should be checked at regular intervals to ensure that it is still accurate. If the information is found to be inaccurate, steps must be taken to rectify it. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded.
Data subjects have a right to access personal data held about them and have inaccuracies corrected.

8. Retention and disposal of Data

GDPR requires that the Parish Council does not keep personal data for any longer than is necessary. Personal data should be checked at regular intervals and deleted or destroyed when it is no longer needed, provided there is no legal or other reason for holding it.
Statutory obligations must be checked before records are disposed of to see whether there is a prescribed retention period for that type of record.

9. Individual Rights

Individuals have several rights under the General Data Protection Regulation. These include the right to access personal data held about them (Subject Access Requests SAR); the right to prevent their information being used in a way which is likely to cause damage or distress; the right to compensation for any damages as a result of their information not being handled in accordance with the General Data Protection Regulation and the right to have inaccurate or misleading information held about them corrected or destroyed; and the “Right to be forgotten”.

It is particularly important that if a person had made a Subject Access request, this is forwarded to the Parish Clerk as soon as possible. The Parish Council has one month in which to respond to a Subject Access request, provided the applicant has put their request in writing and suitable identification has been supplied

10. Closed Circuit Television (CCTV)

Guidance on the use of CCTV and the personal data that it acquires is provided by the Information Commissioners Office (ICO). St Enoder Parish Council operates a CCTV system that is designed to contribute towards enhancing community safety and protect Parish Council property. It is intended therefore that any images available will be viewed (and potentially downloaded) by or at the request of the police force in relation to reported crime or informed crime prevention. Images from the CCTV are retained for up to a month and then automatically deleted.

11. Reporting Data Security Incidents

St Enoder Parish Council has a responsibility to monitor all data security incidents that occur within the organisation that may breach the security and/or confidentiality of its information. All incidents need to be identified, reported, investigated and monitored.