Data Protection Policy and Data Breach Procedure

This policy was formally adopted by

St Cleer Parish Council

on

26.11.25

Review Date 26.11.28

Contents

St CLEER PARISH COUNCIL

DATA PROTECTION POLICY

1 Introduction

1.1 St Cleer Parish Council has a responsibility under 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 is a statement of what the Parish Council does to ensure its compliance with the Act.

1.2 The Data Protection Policy applies to all St Cleer Parish Council employees, Councillors, volunteers, and contractors. The Policy provides a framework within which the Parish Council will ensure compliance with the requirements of the Act and will underpin any operational procedures and activities connected with the implementation of the Act.

2 Background

2.1 The Data Protection Act 2018 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.

2.2 Some of the main features of the Act are:

- All data covered by the Act must be handled in accordance with the Six Data Protection Principles (see Appendix 1)

- 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 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.

- 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.

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

3 Policy Statement

3.1 The Parish Council is committed to ensuring that personal information is handled in a secure and confidential manner in accordance with its obligations under the Data Protection Act 2018 and professional guidelines. The Parish Council will use all appropriate and necessary means at its disposal to comply with the Data Protection Act and associated guidance.

4 Roles and Responsibilities

4.1 Data Protection Officer

4.1.1 The Data Protection Officer is Paul Russell and he is responsible for the following tasks;

4.1.2 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;

4.1.3 Providing advice and monitoring for the carrying out of a data protection impact assessments;

4.1.4 Co-operating with the Information Commissioner's Office, acting as the contact point for the Information Commissioner's Office monitoring compliance with policies of the Parish Council in relation to the protection of personal data monitoring compliance by the Parish Council with the legislation.

4.1.5 In relation to the policies mentioned above, the data protection officer's tasks include:-
(a) assigning responsibilities under those policies,
(b) raising awareness of those policies,
(c) training staff involved in processing operations, and
(d) conducting audits required under those policies.

4.1.6 The Parish Council must provide 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.

4.2 Parish Council

4.2.1 The Parish Council will be responsible for ensuring that the organisation complies with its responsibilities under the Data Protection Act through monitoring of activities and incidents via reporting by the Data Protection Officer. The Parish Council will also ensure that there are adequate resources to support the work outlined in this policy to ensure compliance with the Data Protection Act.

4.3 All Staff and Councillors

4.3.1 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.

4.4 Contractors and Employment Agencies

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 Data Protection Act.

4.5 Volunteers

All volunteers are bound by the same code of behaviour as Parish Council members of staff and Councillors in relation to the Data Protection Act.

5 Records Management

5.1 Good records management practice plays a pivotal role 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 the Act. All records should be retained and disposed of in accordance with the Parish Council retention schedule.

6 Consent

6.1 The Parish Council will take all reasonable steps to ensure that service users, members of staff, volunteers, 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.

6.2 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 Act.

6.3 Should the Parish Council wish to share personal data with anyone other that 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.

7 Accuracy and Data Quality

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

7.2 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.

7.3 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.

8 Data Protection Impact Assessments

8.1 A data protection impact assessment 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 early stages of projects and are embedded in to the Parish Council's decision making process.

9 Providers

9.1 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.

10 Complaints

10.1 Any expression of dissatisfaction from an employee or councillor with reference to the Parish Council's handling of personal information will be treated as a complaint, and handled under the Parish Council's complaint's processes. The Data Protection Officer will be involved in responding to the complaint.

10.2 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.

10.3 We encourage members of the public to use our internal disputes procedure, but this is not mandatory as members of the public can go straight to the Information Commissioner's Office.

11 Security and Confidentiality

11.1 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. Upon employment / date of taking office, staff / councillors must confirm that devices used for Parish Council have adequate security, be password protected, and used solely by the Parish Council staff member / councillor. Paper records must be kept securely.

11.2 The Parish Council 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 Information Commissioner.

11.3. When staff / a councillor leaves the council, they must permanently delete all parish council-related information from personal devices, and ensure paper records are disposed of securely in accordance with best practices for data destruction. The clerk will seek to obtain confirmation of this

12 Rights of Data Subjects

12.1 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 Data Protection Act. Further information on this is available in a separate document, *How to access your records* which can be found on the Parish Council website

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

APPENDIX 1

DATA PROTECTION PRINCIPLES

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 purposes 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, 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;

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.

Data Breach Procedure

1. INTRODUCTION

1.1 We have a responsibility to ensure that personal information is kept and used securely. If anything goes wrong and, for example, data is lost, stolen, misused, sent to the wrong address or inappropriately accessed or released, we equally have a responsibility to put things right.

1.2 All suspected information security incidents must be reported to the Data Protection Officer (DPO). This enables the DPO to conduct a full investigation, and to identify areas of weakness and improvements that need to be made. It also enables the DPO to take a decision as to whether the incident should be reported to the Information Commissioner's Office as a data breach. The latter must be done within 72 hours of discovery, therefore all suspected incidents must be reported to the DPO as soon as they are discovered.

1.3 When sensitive information has been put at risk, but has not actually been lost, stolen, misused or inappropriately accessed or released, it may not be an incident requiring reporting to the Information Commissioner's Office however it is not good practice. For example, a member of staff taking sensitive information home without authority but returning it safely the next day would have put data at risk. The DPO will still put measures in place to prevent a reoccurrence.

1.4 All staff and councillors must be made aware of this procedure.

2. PROCEDURE

2.1 All identified incidents must be reported to the DPO as soon as they are detected. Even where there is some difference of opinion regarding breach, err on the side of caution and report it.

2.2 Upon detecting a breach, it is important to act quickly. In particular it is important to let the DPO know the following:

- The extent of the breach
- The amount of information involved
- The sensitivity of information involved

2.3 The DPO will investigate the incident and establish why it happened, whether or not it constitutes a breach and what remedial action is necessary.

2.4 The DPO will use their initial assessment to report the breach if it meets the necessary threshold for reporting to the Information Commissioner's Office within 72 hours of the discovery of the breach. If this is done after 72 hours, the DPO will provide an explanation for this.

2.5 The DPO will prepare an incident report containing the following:

- A timeline of dates and times concerning the incident

- The potential for loss or damage to individuals, the parish council or any other body
- What measures need to be taken and how quickly to address:-

i. Restoring any lost information to our custody or control

ii. Whether to warn people about the loss, including who to warn and when. This may require a risk assessment.

iii. Factors taken into account for deciding to report the loss to the Information Commissioner's Office.

iv. Whether to report the loss to the Police.

2.6 The DPO will consider taking statements from those involved, especially where the quality of evidence may be lost through time or people may not be present for long.

2.7 The DPO will report any actions that need to be taken to prevent a reoccurrence of the breach and the parish council will ensure that these are implemented.

2.8 The DPO will write to any data subject(s) affected, if necessary dependant on the outcome of a risk assessment, and deal with any subsequent complaint. A standard letter template for this is in Appendix 1.

2.9 The DPO will also correspond as applicable with any member of the public reporting a breach.

2.10 The DPO will deal with any correspondence from the Information Commissioner's Office, providing any further information requested and implementing any recommendations.

APPENDIX 1

Letter to notify that personal data has been breached

I write to you to bring to your attention a breach of the Data Protection Act that unfortunately involves your personal data.

As you would imagine we have taken this matter very seriously and *are investigating the matter / have concluded our investigation into it.*

The facts