# Coddenham Parish Council

# Data Protection Policy

# (GDPR Compliant)

## Introduction

This Policy applies to the processing of personal data in manual and electronic records kept by the Parish Council in connection with its functions as described below. It also covers the Parish Council's response to any data breach and other rights under the General Data Protection Regulation.

This Policy sets out how we seek to protect personal data and ensure that Councillors and Officers understand the rules governing their use of personal data to which they have access to in the course of their work. In particular, this Policy requires Councillors to ensure that the Data Protection Controller be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

We hold personal data about our employees, residents, suppliers and other individuals for a variety of Council purposes.

## Definitions

| | |
|---|---|
| **"Business/ Council purposes"** | The purposes for which personal data may be used by us:<br><br>Personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes.<br><br>*Council purposes include the following:*<br>- *Compliance with our legal, regulatory and corporate governance obligations and good practice*<br>- *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests*<br>- *Ensuring Council policies are adhered to (such as policies covering email and internet use)*<br>- *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting and checking*<br>- *Investigating complaints*<br>- *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments*<br>- *Monitoring staff conduct, disciplinary matters*<br>- *Promoting Council services*<br>- *Improving services* |

| | |
|---|---|
| **"Personal data"** | Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts, members of the public, Council service users, residents, hirers, correspondents<br><br>*Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, contact details, correspondence, emails, databases, council records* |
| **"Sensitive personal data"** | *Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.* |
| **"Data Processing"** | *Data processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.* |
| **"Criminal Offence date"** | *Criminal Offence data is data which relates to an individual's criminal convictions and offences.* |

The Parish Council makes a commitment to ensuring that personal data, including sensitive personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and that all its employees conduct themselves in line with this, and other related policies. Where third parties process data on behalf of the Parish Council, the Parish Council will ensure that the third party takes such measures in order to maintain the Parish Council's commitment to protecting data. In line with GDPR, the Parish Council understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Relevant individuals should refer to the Parish Council's Privacy Notice for more information on the reasons for its processing activities, the lawful basis it relies on for processing and data retention periods.

## Data Protection Principle

All personal data obtained and held by the Parish Council will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purpose of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay

- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

## Procedures

The Parish Council has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:
    a. the processing and controlling of data
    b. the comprehensive reviewing and auditing of its data protection systems and procedures
    c. overviewing the effectiveness and integrity of all the data that must be protected.

    There are clear lines of responsibility and accountability for these different roles.
- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this and to understand how to treat information confidentially
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the Parish Council
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Parish Council understands that consent must be freely given, specific, informed and unambiguous. The Parish Council will seek consent on a specific and individual basis where appropriate. Full information will

be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences
- it is aware of the implications international transfer of personal data internationally.

## Access to Data (Subject Access Requests - SAR)

Relevant individuals have a right to be informed whether the Parish Council processes personal data relating to them and to access the data that the Parish Council holds about them (subject to certain exceptions). Requests for access to this data will be dealt with under the following summary guidelines:

- a form on which to make a subject access request is available from the Parish Clerk. The request should be made to Coddenham Parish Council
- the Parish Council will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the individual making the request
- the Parish Council will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the Parish Council immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Parish Council will take immediate steps to rectify the error.

For further information on making a subject access request, please consult with the Parish Clerk.

## Data Disclosures

The Parish Council may be required to disclose certain data / information to any person. The circumstances leading to such disclosure include:

- any employee benefits operated by third parties
- disables individuals – whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration – to consider how an individuals' health affects their ability to do their job
- The smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

## Data Security

The Parish Council adopts procedures designed to maintain security of data when it is stored and transported. In addition, individuals must:

- ensure that files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- always use passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use
- data stored on computers must be protected by security software.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the Parish Clerk.
Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system – a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

In cases where data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.

Failure to follow the Parish Council's rules on data security may be dealt with via the Parish Council's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

## International Data Transfers

The Parish Council does not transfer personal data to any recipients outside of the EEA.

## Breach Notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Parish Council becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the Parish Council will do so without undue delay.

## Training

New employees must read and understand the policies on data protection as part of their induction.
All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller / auditors / protection officers for the Parish Council are trained appropriately in their roles under the GDPR.

All employees who need to use the Parish Council's computer are trained to protect individual's private data, to ensure data security, and to understand the consequences to them as individuals and the Parish Council of any potential lapses and breaches of the Parish Council's policies and procedures.

## Records

The Parish Council keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities but must not be retained for longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained. Determination will be in a manner consistent with our data retention guidelines.

## Data Protection Compliance

Under legislation, the Parish Council is exempt from the requirement to appoint a Data Protection Officer. The Parish Clerk is the Parish Council's appointed compliance officer, data controller and data processor.

The Parish Council takes compliance with this policy very seriously, Failure to comply puts both you and the Parish Council at risk.
The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Parish Clerk.
We may supplement or amend this policy by additional policies and guidelines from time to time.