FOUR MARKS PARISH COUNCIL
DATA PROTECTION POLICY

Four Marks Parish Council recognises its responsibility to comply with the Data Protection Act 1998 ("the Act") and the General Data Protection Regulations 2018 ("GDPR"). The Act/GDPR regulate the use of personal data. This does not have to be sensitive data, it can be as little as a name and address.

The Act/GDPR set 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. The Act/GDPR apply to anyone holding personal information about people, electronically or on paper.

Anyone who obtains personal information or data about other individuals is a 'data controller' and is thus regulated by the Act/GDPR and controls what can lawfully be done with that information.

The Act/GDPR also gives individuals certain rights to control how information about them is obtained, used, stored and distributed. These rights include the right to find out what information a data controller has about employees and ask for copies of data.

Four Marks Parish Council ("the Council") is the 'data controller' in relation to all the information obtained about employees as part of the process of providing employment.

In order to manage the Council's business, records are kept about employees that necessarily includes the following information:

- Name
- Date of birth
- Sex
- Address
- Next of kin
- Sickness record
- Disciplinary record
- Curriculum Vitae (CV)
- References
- Qualifications
- Rate of pay
- Bank details (if applicable)
- Performance record
- Appraisals
- Criminal records

It is a requirement under the Act/GDPR that employees consent to Four Marks Parish Council processing data about them. Some data is referred to in the Act/GDPR as 'sensitive personal data'. This means personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his/her political opinions
- his/her religious beliefs or other beliefs of a similar nature
- whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- his/her physical or mental health or condition
- his/her sexual life
- the commission or alleged commission by him/her of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

The Council requires that employees expressly consent in their contract of employment to its processing data including sensitive personal data about them. Without this consent it is not necessarily lawful for the Council to process data, in order to keep the records about employees' employment necessary for the Council to meet the needs of conducting its business.

Below is a summary of the legal obligations imposed upon the Council and the rights that employees have under the Act/GDPR, together with the Council's policies about those rights and obligations. The Act/GDPR contain transition periods under which its terms become fully effective over a period of years, however the Council's policy assumes that the Act/GDPR are fully in force.

The Council's Obligations

When dealing with personal data, the Clerk (as the data processor) or designated Councillor (data controller) must ensure that:

- Data is processed fairly and lawfully.
    - This means that personal information should only be collected from individuals if the Clerk and Councillors have been open and honest about why they want the personal information.
- Data is processed for specified purposes only.
- Data is adequate, relevant and not excessive.
    - 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
    - Personal data should be accurate, if it is not it should be corrected.
- Data is not kept longer than is necessary
    - Data no longer needed will be shredded or securely disposed of
- Data is processed in accordance with the data subject's rights
    - Individuals must be informed, upon request, of all the personal information held about them.
- Data is kept securely
    - Only the Clerk, or designated Councillor, can access the data. It cannot be accessed by members of the public

The Council is committed to following these principles and that is why employees must give their consent so that all the Council's data processing in relation to data of which employees are the subject is lawful.

The Council will process data about employees only so far as is necessary for the purpose of managing its business. Data will not be disclosed to anyone else other than the Council's authorised employees, agents, contractors or advisors (except as required by law) unless employees expressly authorise its disclosure. The Council will only obtain data about employees which is required for the managing of its business and dealing with them as employees of the Council.

The Council will take all reasonable steps to ensure that the data processed is accurate. Data will be retained as necessary during the course of an employee's employment and records will be retained for up to seven years after the date that an employee leaves the Council's employment, in case legal proceedings arise during that period. Data will only be retained for a period of longer than seven years if it is material to legal proceedings or should otherwise be retained in the Council's interests after that period.

The Council recognises its responsibility to be open with people when taking personal details from them. The Council may hold personal information about individuals such as their addresses and telephone numbers. These will be securely kept, to the best of the Council's ability, at the Parish Office and are not available for public access. All data stored on the Parish Office computers is password protected. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of our document retention policy, it will be shredded or securely deleted from the computer, as is applicable.

The Council will process data in accordance with employees' rights under the Act/GDPR.

Employees Rights under the Act/GDPR

The Act/GDPR give employees the following rights as a data subject:

1. Access to Data

- To be told whether personal data on themselves is being processed by requesting this in writing.
- To be given a description of the data and its recipients and to have a copy of the data without undue delay and within one month. Confidential references given by the Council are excluded from disclosure (but not necessarily references given **to** the Council). Employees are entitled to know the source of the data.
- The copy should be intelligible and in a permanent form unless to provide it in this form is impossible or would involve disproportionate effort or the employee agrees to accept a non-permanent 'copy'.
- If the data controller has previously complied with a request from an employee then no duty to comply with the request arises until a 'reasonable interval' has elapsed between the two. What will constitute a 'reasonable interval' will depend on the nature of the data, why it is processed and the frequency with which it alters.
- To be informed about the logic used to make automated decisions using the data. For example, some employers will scan CVs submitted for certain information in order to select candidates for further consideration and this right would entitle the candidate to

know what the criteria used was, unless this would necessitate divulgence of a trade secret.

- The request for access to data must be made in writing if the data controller so requires. Employees must provide the data controller with any information reasonably requested to enable the data controller to be satisfied as to the data subject's identity and in order to locate the information.
- Where disclosure of data would necessarily mean that information relating to a third party would be disclosed, the data controller may refuse to disclose it unless the third party consents or it is reasonable to disclose the information without such consent.

2. Rectification of Data

Employees can apply to a court for an order that the data controller rectify, block, erase or destroy inaccurate data and where the court considers it reasonably practicable to do so, inform third parties to whom the data has been disclosed of the fact.

3. Compensation

Should an employee suffer damage as a result of the data controller to comply with the Act/GDPR, he/she may be awarded compensation. Where a data subject suffers distress in certain types of case, there may also be an award of compensation for distress as well as damage.

It is a defence in any claim for compensation that the data controller used such care as was reasonably required in all the circumstances to comply with the Act/GDPR.

4. Information

The Act/GDPR provide that data will not be fairly processed unless the data controller ensures that as far as reasonably practicable the data subject has or has ready access to:

- the identity of the data controller
- any representative of the data controller
- the purpose(s) for which the data is intended to be processed
- any other information necessary to enable the processing to be fair

The Council has incorporated this information in employees' contracts of employment or otherwise given them notice containing this information, including this policy.

However, any data subject whose employer has not notified the Office of the Information Controller that it is a data controller and had these details entered in the public register is entitled to be given (within 21 days of making a written request) 'relevant particulars', which are:

- the data controller's name and address
- the name and address of any representative of the data controller
- a description of the personal data being or to be processed and the category of data subjects to which they relate
- a description of the intended purpose of the processing
- a description of the intended recipients of the data
- a list of the countries outside the European Union that will or may be in receipt of the data from the data controller.
-

5. Direct Marketing

Employees have the right to require in writing that the data controller, within a reasonable time, cease, or not begin processing data of which he/she is the subject for the purpose of direct marketing. Failure to comply by the data controller can lead to a court order that the data controller does so.

6. Right to Stop Data Processing

Employees have the right to require that a data controller cease or not begin data processing where the processing is causing or likely to cause unwarranted and substantial damage or unwarranted or substantial distress to them or another by giving notice in writing, specifying why the data processing is or will be the cause of distress or damage and the purpose and manner of processing to which objection is made. The data controller then has to respond with a written notice, within one month unless good reason, stating either that they have or intend to comply with the request, or why they regard the notice as unjustified and the extent to which they have, or intend to comply with it. Employees can make application to the court if the data controller does not comply.

However, where the employee has consented to the data processing or it is necessary for the performance of a contract to which they are a party and the data controller requests it with a view to entering into a contract, or the data controller has a non-contractual legal obligation which requires them to carry it out, the employee has no right under this section to stop the data processing.

The Council's Policy on Access to Data

1. A request for access to any personal data that relates to employees should be made by a written request.
2. On receipt of a request it is the Council's policy to provide copies of all data which the Council is obliged to disclose **within one month, unless good reason**, receipt of a request by the data protection compliance officer of the Council.
3. The Council considers that if a period of less than one year has elapsed since any previous request for access to data was complied with, it is not reasonable to expect the Council to be obliged to comply with a further request before a year has elapsed, unless there are exceptional circumstances.
4. Should an employee wish to bring any inaccuracy in disclosed data to the Council's attention, the employee must do this in writing. In appropriate circumstances, employees may find that arranging an appointment to hand a written notification of any inaccurate data to the Council, is preferable.
5. It is the Council's policy to ensure that all data is as accurate as possible and all necessary steps to ensure that this is the case and to rectify any inaccuracies will be taken.

Where the Council has requested a reference in confidence from a referee and that reference has been given on terms that it is confidential and that the person giving it wishes that it should not be disclosed to the employee, it is the Council's policy that it would normally be unreasonable to disclose such a reference to an employee, unless the consent of the person who gave the reference is obtained.

Confidentiality

The Clerk, Chairman and Councillors must be aware that when complaints or queries are made, they must remain confidential unless the data subject gives permission otherwise. When handling personal data, this must also remain confidential.

Data Processor: **The Executive Officer**
Data Controller: **The Council**