Fowlmere Parish Council

Data Protection (GDPR) Policy
Cover Page

This Data Protection (GDPR) Policy was adopted by Fowlmere Parish Council on 20th November 2018.

Review Date	Reviewed by	Review accepted by Full Council
16th May 2023	Full Council	16th May 2023
21st May 2024	Full Council	21st May 2024
20th May 2025	Full Council	20th May 2025
next review May 2026		

Fowlmere Parish Council

DATA PROTECTION POLICY

Adopted 20th November 2018

1. ORGANISATION

This policy applies to Fowlmere Parish Council.

2. INTRODUCTION

This Data Protection Policy sets out how Fowlmere Parish Council ("we", "our", "us", "the Council") handle the Personal Data of our parishioners, suppliers, employees, workers and other third parties.

This Data Protection Policy applies to all Personal Data we use in any way regardless of the media on which that data is stored.

This Data Protection Policy applies to all Council Personnel – both Officers and Councillors ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for the Council to comply with applicable law when using Personal Data for any purpose, including discharge of the Council's statutory functions and powers, internal Council purposes, and all related activities. Your compliance with this Data Protection Policy is mandatory. If you have questions about this Data Protection Policy or its application please contact the Parish Clerk. Any breach of this Data Protection Policy may result in disciplinary action.

Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a Data Protection Impact Assessment (DPIA) as referenced in this Data Protection Policy or otherwise then you must comply with the Related Policies and any provided guidelines.

This Data Protection Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Parish Clerk.

3. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in Fowlmere Parish Council. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. We are exposed to potential fines of up to EUR20 million (approximately £18 million) for failure to comply with the provisions of the GDPR.

All individuals are responsible for ensuring that all Council Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Clerk, with the support of the Chairman of the Finance Committee is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and guidelines.

Please contact the Clerk with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the Clerk in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the necessity of the Processing for the Public Tasks executed by the Council) (see *Paragraph 5.1* below);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see *Paragraph 5.2* below);

(c) if you need to draft Privacy Notices (see *Paragraph 5.3* below);

(d) if you are unsure about the retention period for the Personal Data being Processed (see *Paragraph 9* below);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see *Paragraph 10.1* below);

(f) if there has been a Personal Data Breach (see *Paragraph 10.2* below);

(g) if you are unsure on what basis to transfer Personal Data outside the EEA (see *Paragraph 11* below);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see *Paragraph 12*);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see *Paragraph 13.4* below) or plan to use Personal Data for purposes others than what it was collected for;

(j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see *Paragraph 13.5* below); or

(k) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see *Paragraph 13.6* below).

4. PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Where applicable, made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1 LAWFULNESS AND FAIRNESS

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) where Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us as the controller;

(b) to meet our legal compliance obligations;

(c) to fulfil our contractual obligations;

(d) to protect the Data Subject's vital interests; or

(e) the Data Subject has given his or her Consent.

You must identify and document the legal ground being relied on for each Processing activity in accordance with our guidance on Lawful Basis. This information must be provided to the Clerk for inclusion in our Processing Register.

5.2 CONSENT

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing.

Data Subjects must be easily able to withdraw Consent to Processing at any time as easily as the consent was originally given. Consent will need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

If you are using Special Categories of Personal Data please discuss this with the Clerk. Explicit Consent is frequently required for Processing Special Categories of Personal Data and Criminal Convictions Data, for Automated Decision-Making and for data transfers outside the EEA. Where Explicit Consent is required, you must issue a Privacy Notice and consent request to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and any provided guidelines so that the Council can demonstrate compliance with Consent requirements. This includes verbal consent that must either be voice recorded or otherwise documented contemporaneously.

5.3 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

If we are making decisions about Personal Data then we are required as the Data Controller to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data unless an exemption exists. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6. PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes. This should be considered carefully both in the context of project design and in the offering of solutions to clients.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7. DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your Council duties requires it. You cannot Process Personal Data held by the Council for any reason unrelated to your Council duties.

You may only collect Personal Data that you require for your Council duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Council's data retention guidelines as documented in the Processing Register.

8. ACCURACY

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted

without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data was processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the Legal Obligation, Public Task or other purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Council will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Council's applicable records, retention schedules and policies. This includes requiring third parties to delete such data, where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

10. SECURITY INTEGRITY AND CONFIDENTIALITY
10.1 PROTECTING PERSONAL DATA

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

You are responsible for protecting the Personal Data we hold. You must exercise particular care in protecting Special Categories of Personal Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. The method of transfer should also be appropriate to the classification of the data.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it

for authorised purposes.

You must comply with all applicable aspects of our Information Security Policy.

10.2 REPORTING A PERSONAL DATA BREACH

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Clerk. You should preserve all evidence relating to the potential Personal Data Breach. There are strict timelines within which breaches must be reported, which in some cases may be as little as 24 hours.

11. TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has confirmed that the country to which we transfer ensures an adequate level of protection;

(b) appropriate safeguards are in place such as standard contractual clauses approved by the European Commission; or

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the

public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling and Automated Decision Making (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

The extent to which these rights can be exercised depends upon the Lawful Basis being used for Processing.

You must immediately forward any Data Subject request you receive to the Clerk.

13. ACCOUNTABILITY

13.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Council must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(b) integrating data protection into internal documents including this Data Protection Policy, Related Policies, guidelines or Privacy Notices;

(c) regularly training Council Personnel on the GDPR, this Data Protection Policy, Related Policies and guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Council must maintain a record of training attendance by Council's Personnel; and

(d) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement efforts.

13.2 RECORD KEEPING

The GDPR requires us to keep full and accurate records for the most frequent of our data Processing activities.

You must keep and maintain accurate records reflecting our Processing including records of Data Subjects'

Consents, privacy Notices issued and procedures for obtaining consent.

These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, in situations involving multiple parties or data sources, data maps should be created which should include the detail set out above together with appropriate data flows.

13.3 TRAINING AND AUDIT

We are required to ensure all Council Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate controls and resources are in place to ensure proper use and protection of Personal Data.

13.4 PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

The Council encourages, where possible, Processing activities to be based upon the principles of Privacy by Design and demonstrating compliance with these will be sufficient for most Processing activities. However, for cases involving high risk Processing it will be necessary to also conduct case-specific DPIAs.

You should conduct a DPIA (and discuss your findings with the Clerk) when implementing major system or change programs involving the Processing of Personal Data including:

(a) Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) Automated Processing including profiling and ADM;

(c) Large scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

(d) Large scale, systematic monitoring of a publicly accessible area.

You must comply with any guidelines provided by the Council on DPIA.

13.5 AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless the Data Subject has Explicitly Consented. If you intend to undertake ADM please contact the Clerk.

13.6 SHARING PERSONAL DATA

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Council Personal Data we hold with another member of Council Personnel if the recipient has a job-related need to know the information and there is no contractual restriction on doing so.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) where the other party has provided sufficient guarantees that it will comply with the provisions of GDPR and a fully executed contract containing GDPR approved third party clauses has been obtained.

14. CHANGES TO THIS DATA PROTECTION POLICY

We reserve the right to change this Data Protection Policy at any time. We will notify all Council Personnel when changes are made.

Terminology

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Council Personnel: all Council employees, workers [contractors, agency workers, consultants], Officers, Councillors and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the controller of all Personal Data relating to our Council Personnel and Personal Data used in undertaking the Council's business.

Criminal Convictions Data: means personal data relating to criminal convictions and offences.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

EEA: the countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Council collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals

(for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Processing Register: the Council's central record of all Processing activities, the data held, why it is being Processed, the legal basis for this, how long it will be kept, where it is held, the controls in place, the extent to which it is shared with other parties, and the arrangements in place to underpin this.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Council's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.