MEDSTEAD PARISH COUNCIL
DATA PROTECTION POLICY

1. Introduction

This Policy is adopted by Medstead Parish Council pursuant to its statutory duty to comply with the UK General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA). This legislation mandates controls on the processing of Personal Data.

The Council collects and uses certain types of personal information about staff, Councillors, residents, volunteers, contractors and other individuals who come into contact with the Council for a variety of business purposes. It may also be required by law to collect and use certain types of information to comply with statutory obligations related to employment.

This policy will be made available to Councillors, staff and, where appropriate, volunteers to ensure that they are aware of the Council requirements for data protection.

2. Data Protection Legislation

2.1 Personal data

'Personal data' is information that relates to an identifiable, living person who can be directly or indirectly identified from that information, for example, a person's name, address, email address, photo, bank details, national insurance number, passport or driving licence number or other identification number and any other information which uniquely identifies an individual (on its own or in conjunction with other information). It can also include pseudonymised data.

There are certain subsets of personal data that are given special protection, and additional safeguards apply if this information is to be collected and used.

- 'Sensitive personal data' is data that relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion or trade union membership. (The definition also includes genetic and biometric data used for ID purposes).
- '*Criminal offence data'* is data that relates to an individual's criminal history.
- *'Children's personal data'* relates to those under the age of 13.

The Council does not intend to seek or hold sensitive personal data except where it has been notified of the information, or it comes to light via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. The Council does not process children's data.

2.2 Data Subject

The '*Data subject*' is the term used for the individual to whom the personal data relates.

2.3 Data processing

'*Data processing'* is any operation or set of operations that are performed on personal data or on sets of personal data. Data processing operations include collection, recording, organisation structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Processing may be by manual or automated means.

The Parish Council processes personal data to enable it to carry out its statutory duties, represent the community of the Parish, provide and promote its services, undertake fundraising, maintain its accounts and records and manage its staff and contractors.

2.4 Principles relating to processing of personal data

Article 5 of the GDPR details seven data protection principles which the Council must adhere to at all times. These are listed below:

i. Fair Lawful and Transparent Processing

All personal data will be processed lawfully, fairly and in a transparent manner in relation to the data subject.

ii. Purpose limitation

It will be clearly specified exactly what the personal data to be collected will be used for and limit the processing of the data to only that which is necessary to meet the explicit, legitimate and specified purpose.

iii. Data minimisation

Personal data will be adequate, relevant and limited to that which is necessary in relation to the purposes for which it is processed, personal data beyond that which is strictly required will not be stored.

iv. Accuracy and relevance

Any personal data processed will be accurate and relevant, not excessive and kept up to date. Inaccurate data will be erased or rectified without delay.

v. Storage limitation, data retention and storing data securely

Wherever possible, personal data will be stored in a way that limits or prevents identification of the data subject. All personal data will be deleted or destroyed as soon as possible where it has been confirmed there is no longer a need to retain it.

vi. Integrity, confidentiality and data security.

Personal data will be processed in a manner that ensures appropriate security of the data including protection against unauthorised or unlawful processing, against accidental loss, destruction or damage using appropriate technical or organisational measures.

vii. Accountability

The Data Controller shall be responsible for and be able to demonstrate compliance with UK GDPR and review and update relevant policies and procedures.

2.5 Lawfulness of processing personal data

Article 6 of the GDPR defines six legal bases for processing personal data. Processing shall be lawful only if and to the extent that at least one of the following applies.

- Consent: The individual has given clear consent for the processing.
- Contract: Processing is necessary for the performance of a contract.
- Legal obligation: Processing is necessary to comply with the law.
- Vital interests: Processing is necessary to protect someone's life.
- Public task: Processing is necessary for a task carried out in the public interest or in the exercise of official authority.

- Legitimate interests: Processing is necessary for the legitimate interests pursued by the controller or a third party, except where overridden by the rights of the data subject.

If in any doubt about the lawful basis for processing information, the Information Commissioner's Officer has a Lawful basis interactive guidance tool | ICO to help.

The Council will ensure that all processing of personal data has a lawful basis.

2.6 Individual's rights.

Personal data must be processed in recognition of an individual's data protection rights as follows:

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

The Council will fulfil all such requests, subject to legal limitations.

2.7 Data controllers and processors

Medstead Parish Council is a Data Controller as defined in the UK GDPR. It defines a controller as:

"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".

Controllers make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing.

The UK GDPR defines a Processor as:

"'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own.

The Council does not routinely process information on behalf of any other body. Where it receives information from other bodies, e.g. electoral register information from EHDC, it determines how to process that information and so is acting as a controller.

3. Council policies and procedures to comply with GDPR legislation

Medstead Parish Council must meet all of the legal obligations, i.e. making sure that it complies with all seven data protection principles, the individual's rights with regard to personal data are all upheld, and all process of personal data processing is done using a valid legal basis and all other requirements of UK GDPR are fulfilled.

The following sections identify all the measures that collectively meet these obligations.

3.1 Records of data processing activity

Medstead Parish Council will keep records of data processing (which must be kept up to date).

Parish Councils are not classed as public bodies in the UK GDPR and the regulations provides a limited exemption for small and medium-sized organisations employing fewer than 250 people, who need only document processing activities that:

- are not occasional (e.g. are more than just a one-off or rare occurrence); or
- are likely to result in a risk to the rights and freedoms of individuals; or
- involve special category data or criminal conviction and offence data

Despite the exemption, the Council will keep records of processing activity as much as it practical as it is important to help the Council do the following:

- identify personal data impacted in the event of a data breach
- ensure personal data has the appropriate level of security
- check that all data processing has a legal basis
- ensure that personal data is not held for longer than is necessary
- justify its approach if sharing personal data
- demonstrate accountability and compliance with UK GDPR, which requires the Council to take responsibility for what it does with personal data

3.2 Designation of roles

The Council collectively has responsibility for complying with the Data Protection Act and UK GDPR and it cannot delegate this responsibility or any decision-making authority to an individual Councillor.

UK GDPR identifies the role of a Data Protection Officer in articles 37-39 but Medstead Parish is not legally required to appoint one as it is not classed as a public authority in this legislation, it does not undertake large scale processing of sensitive personal data and it does not engage in "regular and systematic monitoring" of individuals on a large scale.

Notwithstanding this, there are elements of the DPO role that are beneficial to a Parish Council, such as having an individual(s) with a level of expertise who can advise and educate the Council and ensure its activities are compliant with UK GDPR and assist should a data breach occur.

The Councillor will appoint two Data Protection Lead Councillors who will have a level of expertise on data protection and undertake training as required. This is in additional to the expertise of the Clerk, and they will be able to fill a vacuum in knowledge should a Clerk vacancy or absence due to ill-health unexpectedly occur or if the Council finds it necessary to recruit an inexperienced Clerk or if there are problems with the Clerk's performance with regards to their compliance with GDPR. By having two lead Councillors, the Council has built in a level of redundancy for continuity should a single Councillor not be available or resigns. These lead Councillors will be appointed at each annual meeting or when a resignation of one of them occurs.

The Clerk will be the day to day lead on data protection, reflected in their job description, and the Clerk will also play a key role in advising the Council on the implications of data protection in its actions, such as when considering a new opportunity.

The Clerk is appointed as the Controller's representative for Medstead Parish Council as referenced in the UK GDPR and will be the name of the person detailed on Privacy Notices.

The Clerk will have ultimate responsibility for making decisions regarding data breaches, including the need to report it to the Information Commissioner's Office and individuals affected. The Data Protection Lead Councillor(s) cannot be delegated this individual responsibility and there is a need to report data breaches to the ICO within 72 hours, whereas there needs to be a three clear days minimum notice to hold a legally-called extraordinary council meeting or committee. However, before investigating a data breach and making

decisions, the Clerk will inform and advise the Chairman, the Data Protection Lead Councillors (and the rest of the Councllors as appropriate), and will take guidance from them.

The appointment of Data Protection Lead Councillors does not absolve the need for all Councillors having an understanding of data protection legislation and share the Council's responsibilities, and this is covered in more detail in the Training Policy. It is simply a pragmatic step to ensure that a level of expertise exists, even if it is not equal in all Councillors, and to ensure that the Councillor can share advice and come to decisions quickly, should the need arise.

The Council collectively has responsibility to adopt policies and procedures that adhere with the GDPR legislation and to keep abreast of new legal requirements, supported and advised by the Clerk and the Data Protection Lead Councillors.

At year end, the Annual Governance Statement Assertion 10 emphasizes the importance of compliance with the UK GDPR and the Data Protection Act. Councils are required to have a clear understanding of the personal data they process, including the purpose, storage, access, sharing and deletion. This involves conducting data audits and risk assessments to ensure compliance with data protection legislation.

3.3 Training Policy

The Council's Training Policy requires that the Clerk has undertaken suitable training in GDPR, and that for a new inexperienced Clerk this should be undertaken as soon as is practical on joining.

At least two Data Protection Lead Councillors (as outlined earlier) will also undertake suitable data protection training, dependent on their starting level of expertise. This does preclude other Councillors also undertaking specialist training as desired / required. The best training to use will be a current decision, kept under ongoing review, dependent on cost, availability, scope and feedback.

All Councillors will undertaken induction training by attending the Knowledge and Core Skills HALC training course and by reading a pack of induction material compiled by the Clerk, which includes information on UK GDPR. All new Councillors must read this Data Protection Policy as part of their induction.

3.4 Privacy Notices

UK GDPR says that where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with the information with is listed in Article 13 of the UK GDPR. Article 14 details the information to be provided where information has not been obtained from a data subject, rather from another source.

Privacy notices should include information on the identity of the organization, reasons for data use, legal grounds for processing, entities with which data may be shared, transfers of data outside the UK, retention period, and data subjects' rights. The Council should consider the presentation and timing of privacy notices, as well as the specific needs and circumstances of their data subjects. To comply with the UK GDPR, privacy notices must be clear, accessible, and regularly reviewed.

UK GDPR says that the requirement for privacy notices can be put on the Council's website, however the Council must proactively make individuals aware of this information and they need to give them an easy way to access it. Simply putting it on your website, in case people happen to look there, is not enough.

Based on this guidance, the Clerk will put a link to privacy information on the email signature, and it will be included on cemetery application forms, job application forms, surveys and any other relevant forms or online information requests.

The Council will publish on its website a general privacy notice, that will cover residents and other members of the public, contractors and volunteers. In some cases, specific notices may be required for contractors and volunteers. The Council will also issue a separate privacy notice to its staff and councillors

3.5 Consent requests

In general, personal information that Medstead Parish Council processes will be based on the other five legal bases rather than consent, due to the nature of Parish Council business.

Where consent is needed, the Council recognises that GDPR requires it to be freely given by an individual and such decisions should be specific, informed and unambiguous. Consent must be positive, and so the Council cannot rely on requests that require the data subject to only reply if they do not consent.

If the Council wants to use personal information for a purpose that exceeds the consent which was originally requested, it will need to get additional consent from the data subject.

The Council will create consent forms tailored to whatever need it has that conform with the principles above and they will be retained electronically or physically for audit purposes in line the data retention policy. Individuals have the absolute right to withdraw that consent at any time.

3.6 Subject access requests

Individuals are entitled to request access to information held about them. Medstead Parish Council will consider each request in accordance with all applicable data protection laws and regulations.

The Council has a separate Subject Access Request Policy that it will follow when it receives any subject access requests.

3.7 Correction and deletion of data

To comply with the principle of accuracy and relevance, Medstead Parish Council aims to ensure that personal data is correct and accurate and is not misleading, incomplete or outdated.

If a data subject requests a change to data or points out a mistake, the Council will act quickly to make the changes and will confirm to the individual that it has been done.

The Council will not wait for individuals to request action and will correct any inaccuracies that it becomes aware of.

The Council will keep personal data only for the period necessary to satisfy the permitted uses or the applicable retention period. It will remove personal data if in violation of any of the data protection principles or if the personal data is no longer required.

When the Council receives a request from a data subject to delete personal data, it needs to consider this in line with the Councils Data Retention Policy as there may be legal requirements for keeping data and it may not be possible to remove it, in which case the data subject will be kept informed.

Employees and Councillors must take responsible steps to ensure that the personal data held about them is accurate and updated as required. This would include changing a name or address.

When deleting physical documents containing personal data, the Council will use a secure means of doing so, such as a cross-shredder that meets the required standards.

3.7 Data Retention Policy

The Council has adopted a Data Retention Policy, which details how long the Council needs to hold different types of information, including personal data, and how it will delete it. The retention periods are dictated by legal requirements, business need and the purposes for which information was provided.

The Council will keep abreast of any relevant changes in legislation to make sure that this policy continues to be fit for purpose.

3.8 Data Breach Policy

UK GDPR outlines steps that the Council should take to avoid data breaches and the measures that it should take should a data breach occur (in Articles 32-24). In the event of a data breach, there can be serious consequences and the Council may need to inform the Information Commissioner's Office and any individuals affected, and this should be done within 72 hours of a data breach occurring. Urgent steps need to be taken to investigate the breach, assess the impact of it and determine the appropriate actions. This is detailed in the separate Data Breach Policy.

3.9 Information Commissioner's Office

As a Data Controller, the Council needs to pay the appropriate fee to the Information Commissioner's Office and display the ICO Certificate on its website. The payment to the ICO is on direct debit, so it is done automatically every year and cannot be overlooked.

The ICO is the UK's independent regulatory body that is responsible for upholding information rights and enforcing data protection laws. It was established to oversee and regulate the implementation of data protection laws in the UK, including the General Data Protection Regulation (GDPR) and the Data Protection Act. It protects individuals' personal data by overseeing organisations' data processing activities and ensuring compliance with the GDPR.

3.10 Physical data security and IT Policy

The Council maintains the security of both physical and electronic data.

Most Council documents are held at the Parish Office where there are triple levels of locks, to both the individual filing cabinets, the store room and the office building itself, and key holders are controlled.

Documents in the Clerk's home will be kept to a minimum and if any are located there whilst working on them, the Clerk's contract of employment dictates the need for them to be locked away when not in use.

Councillors will be made aware through induction information and through this policy of the need to safeguard the confidentiality and security of any Council documents they may hold. However, most printed material Councillors choose to hold will the documents in the public domain such as minutes and agendas.

The Council must safeguard any online information that it holds against loss, theft or data breaches and has adopted an IT Policy that covers this requirement.

3.11 Data disclosures and transfers

The Council may disclose or transfer personal data to internal or third-party recipients. The circumstances leading to such a disclosure include sending information to:

- Other third parties who provide services to the Council, i.e. pensions providers, HMRC or potentially a payroll provider.

- Where there is a legal obligation to do so, for example, where there is a requirement to share information under statute to prevent fraud and other criminal offences. This may be in the form of a court order from the police or HMRC.

Before sharing information with another organisation, the Council must consider the following factors:

- It must be clear about the specific purpose for sharing information. The Council will need to record its purposes and specify them in the Council's privacy information to individuals. It must identify the lawful basis for sharing the information.
- The Council should inform individuals that their information has been shared. This can be via a privacy statement on the website, but individuals should be made aware of it and given easy access to it.

The Council does not transfer personal data outside of the UK.

3.12 Risk Assessment and mitigation

The Council will complete risk assessments for all new activities and will review its existing risk assessments at least one a year. This must include an assessment of risks to personal data and mitigating measures to reduce the risks.

3.13 Information in the public domain

The Council will not publicly identify any residents or other individuals in the minutes or agendas or other public documents on the website unless they specifically request it (in which case the Clerk will follow up with them on email to get their consent). This excludes contractors who need to be made public for other statutory reasons.

3.14 Information voluntarily provided to the Council

If someone voluntarily emails or phones the Council and also provides personal information, such as a name, consent is not specifically needed as the personal data is needed for another lawful purpose, e.g. public task, legitimate interest etc, to deal with a complaint, query etc. However, this information should not be forwarded to anyone outside the Council without permission and it should be retained no longer than is deemed necessary in the Data Retention Policy or used for a different purpose.

Version Control

Version	Date adopted	Minute ref.
Data Protection Policy 2026	First adopted 22nd January 2026	26.013(a)