Meppershall Parish Council

DATA PROTECTION POLICY

As adopted at a meeting of Meppershall Parish Council on ***10th December 2018***

CONTENTS

Organisation	Meppershall Parish Council
Title	MPC Data Protection Policy
Creator	Alessandra Marabese - Clerk
Source	Procedures Working Group
Approvals	Monday 10th December 2018
Distribution	Internal and External
Filename	MPC Data Protection Policy v2.0 2018©
Owner	Clerk
Subject	Data Protection
Protective Marking	None
Review date	Annually after adoption

DOCUMENT AMENDMENAT HISTORY

Revision No.	Originator of change	Date of change	Change Description
2.0	Clerk	10/12/18	Policy re-write

1. INTRODUCTION

1.1. **Meppershall Parish Council** (the Council) holds personal data about employees, residents, suppliers and other individuals for a variety of Council purposes.

1.2. This policy sets out how we seek to protect personal data and ensure that those acting on the Council's behalf understand the rules governing the use of personal data to which they have access in the course of their work. In particular, this policy requires Officers to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

1.3. The Council will ensure that personal information is treated lawfully and correctly, adhering always to the principles of the Data Protection Act 2018 and any subsequent revisions.

1.4. As a 'data controller', the Council has also notified the Information Commissioner's Office (ICO) that it holds personal data about individuals.

2. SCOPE

2.1. This policy applies to all councillors, employees and third parties acting on behalf of the Council who must be familiar with this policy and comply with its terms.

2.2. The Council may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be made available to councillors, employees and third parties.

3. THE DATA PROTECTION ACT 2018

3.1. The Data Protection Act 2018 (the Act) establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes, against the right of individuals, known as 'data subjects' to respect for the privacy of their personal details. This is underpinned by eight principles:

3.1.1. Personal data shall be processed fairly and lawfully – this means that personal information must only be collected from individuals in an open and honest manner with the data subject being made aware of why the information is required.

3.1.2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3.1.3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

3.1.4. Personal data shall be accurate and, where necessary, kept up-to-date.

3.1.5. Personal data shall not be kept for longer than is necessary and will be securely shredded or disposed of.

3.1.6. Personal data shall be processed in accordance with the rights of data subjects. Individuals must be informed, upon request, of all the personal information held on them.

3.1.7. Data is kept securely. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

3.1.8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.2. As part of its role, the Council is required to gather and process information about people in the community in order to operate effectively. This will be carried out in accordance with the Data Protection Act 2018 and other related government legislation. This information may also be shared with other agencies involved in the provision of services, where the Council is legally required to do so.

3.3. Personal data will only be processed and held where there is one of the following reasons (lawful basis) to do so:

3.3.1. Consent – Data given freely for a specific purpose

3.3.2. Contractual – Data required to fulfil contractual obligations

3.3.3. Legal obligations – Data is required to comply with a common law or statutory obligation

3.3.4. Vital Interest – Data is required to protect the vital interests of an individual

3.3.5. Public Task – Data is required in the exercise of official authority or to perform a specific task in the public interest that is set out in law

3.3.6. Legitimate interest – Data is required for the legitimate interests of the Council or third party, if it does not conflict with the rights of the individual.

4. ROLES AND RESPONSIBILLITIES

4.1. The Data Protection Officer's Responsibilities:

4.1.1. Keeping the Council updated about data protection responsibilities, risks and issues.

4.1.2. Reviewing all data protection procedures and policies on a regular basis.

4.1.3. Assisting with data protection training and advice for all staff members and those included in this policy.

4.1.4. Answering questions on data protection from staff, council members and other stakeholders

4.1.5. Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them by the Council.

4.1.6. Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing.

4.2. Responsibilities of the Clerk:

4.2.1. Ensure all systems, services, software and equipment meet acceptable security standards.

4.2.2. Checking and scanning security hardware and software regularly to ensure it is functioning properly.

4.2.3. Researching third-party services, such as cloud services the Council is considering using to store or process data.

4.2.4. Approving data protection statements attached to emails and other marketing copy.

4.2.5. Addressing data protection queries individuals or media outlets.

5. OUR PROCEDURES

5.1. The processing of all data must be;

5.1.1. necessary to deliver our services,

5.1.2. in our legitimate interests and not unduly prejudice the individual's privacy.

In most cases this provision will apply to routine business data processing activities.

5.2. The Council's Privacy Notice;

5.2.1. sets out the purposes for which we hold personal data on customers, employees, residents and service users,

5.2.2. highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers,

5.2.3. provides that service users and correspondents have a right of access to the personal data that we hold about them.

5.3. Sensitive personal data

5.3.1. In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with burial legislation and allotment legislation). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

5.4. Accuracy and Relevance

5.4.1. We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

5.4.2. Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and request rectification.

5.5. Your personal data

5.5.1. You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the DPO so that they can update your records.

5.6. Storing data securely

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

5.6.2. Printed data should be shredded when it is no longer needed

5.6.3. Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.

5.6.4. Data stored on CDs or memory sticks must be locked away securely when they are not being used.

5.6.5. Servers containing personal data must be kept in a secure location, away from general office space.

5.6.6. Data should be regularly backed up in line with the council's backup procedures.

5.6.7. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

5.6.8. All servers containing sensitive data must be approved and protected by security software and strong firewall.

5.7. Data retention

5.7.1. We must retain personal data for no 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, but should be determined in a manner consistent with our data retention guidelines.

5.8. Training

5.8.1. All councillors, employees and appropriate third parties will receive training on this policy. Further training will be provided whenever there is a substantial change in the law or our policy and procedure.

5.8.2. Training is provided through an in-house seminar. Completion of training is mandatory.

5.9. Data audit and register

5.9.1. Regular data audits to manage and mitigate risks will aid to update the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

5.10. Reporting breaches

5.10.1. All councillors, employees and relevant third parties have an obligation to report actual or potential data protection compliance failures to the DPO. This allows us to:

5.10.1.1. Investigate the failure and take remedial steps if necessary

5.10.1.2. Maintain a register of compliance failures

5.10.1.3. Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

5.11. Monitoring

5.11.1. The Council have appointed a DPO who is responsible for monitoring and maintaining compliance. The Council support the DPO by consistently monitoring for vulnerabilities, breaches, withdrawal of consent, and other issues that could lead to non-compliance.

6. RIGHTS OF DATA SUBJECTS

6.1. The Council has a responsibility to ensure that data subjects have appropriate access, upon written request, to details regarding personal information relating to them.

6.2. Data subjects have;

6.2.1. the right to be informed about the collection of personal data,

6.2.2. the right of access to data that is the Council holds on them,

6.2.3. the right to rectification is data is inaccurate,

6.2.4. the right to erasure of personal data,

6.2.5. the right to restrict processing or suppression of personal data,

6.2.6. the right to data portability allowing individuals to obtain and reuse their personal data for their own purposes across different services,

6.2.7. the right to object the processing of personal data in certain circumstances,

6.2.8. rights related to automated decision making and profiling in certain circumstances.

6.3. If a data subject wishes to see the personal information the Council holds on them, they should write to the Council addressing correspondence to the Clerk by e-mail: *clerk@meppershall.org or by post to 30 Cherry Trees, Lower Stondon, Bedfordshire, SG16 6DT.*

6.3.1. To ensure that information is released to the correct data subject concerned, there will be a need to provide proof of identity.

6.3.2. The Council does not make a charge for requesting the information.

6.4. Once requested, the Council is obliged to provide the information within 40 days of receiving the written application.

6.5. If the data held is incorrect, data subjects can request that it be corrected, and this must be in writing or by e-mail, unless the data subject has a disability which would prevent this or make it unreasonably difficult for them. Such information must be corrected within 28 days of the request to make the amendment. If the correction is not made, the data subject can appeal to the ICO.

7. DISCLOSURE OF PERSONAL INFORMATION

7.1. If a Councillor needs to access information to help carry out their duties, this is acceptable. They are only able to access as much information as is necessary and it should only be used for that specific purpose. If, for instance, someone has made a complaint about over hanging bushes in a garden, a Councillor may access an address and telephone number of the person who has made the complaint, so they can help with the enquiry. A councillor may only do this providing they represent the area that the subject lives in. However, before they access any sensitive information about a person, they would need consent to do this from the Clerk. Data should never be used for political reasons unless the data subjects have consented.

8. COMPLAINTS

8.1. The Council takes compliance with this policy very seriously. The importance of this policy means that failure to comply with any requirement may lead to serious action.

8.2. If data subjects have a complaint regarding the way personal data has been processed by The Council, they may make a complaint to the Council's DPO *Jayne Cole, Chief Executive Officer, Local Council Public Advisory Service, The Vision Centre, 5 Eastern Way, Bury St Edmunds, Suffolk, IP32 7AB, Tel: 01284 766885.*

8.3. If data subjects are dissatisfied about any matter, they can complain to the ICO. Complaints can be made if a data subject considers the Council or the Council's DPO has breached any of the requirements of the Data Protection Act 2018 and these include the following, but the list is not exhaustive:

- A breach of data protection principles.
- Processing personal data without having notified the Commissioner.
- Failure to respond to any of the data subject's written notices.
- Processing personal data without a data subject's consent, where consent is necessary.
- refusing to provide a data subject with the information requested.

The Commissioner will carry out an assessment of the Council's processing to establish whether the Council has complied with the Act. If the finding is that the Council has not complied, the Council will be issued with a notice requiring compliance. The ICO's contact details are: *Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel: 0303 123 1113. Alternatively, visit the ICO's website or email casework@ico.org.uk*

9. CONFIDENTIALITY

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