

## **2. DATA PROTECTION POLICY (AND INFORMATION SECURITY)**

- 2.1. Mepal Parish Council hold personal data about our employees, residents, suppliers and other individuals for a variety of Council purposes.
- 2.2. 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 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.
- 2.3. This policy applies to all councillors and staff.
- 2.4. The Data Protection Officer, [Parish Council Clerk] has overall responsibility for the day-to-day implementation of this policy
- 2.5. All personal data must be processed fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.
- 2.6. The Data Protection Officer's responsibilities are:
  - 2.6..1. Keeping the Council updated about data protection responsibilities, risks and issues
  - 2.6..2. Reviewing all data protection procedures and policies on a regular basis
  - 2.6..3. Assisting with data protection training and advice for all staff members and those included in this policy
  - 2.6..4. Answering questions on data protection from staff, council members and other stakeholders
  - 2.6..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 Mepal Parish Council
  - 2.6..6. Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing
- 2.7. The Clerk acting at the IT Manager is responsible for:
  - 2.7..1. Ensuring all systems, services, software and equipment meet acceptable security standards
  - 2.7..2. Checking and scanning security hardware and software regularly to ensure it is functioning properly
  - 2.7..3. Researching third-party services, such as cloud services the company is considering using to store or process data
- 2.8. The Clerk is responsible for:

- 2.8..1.Approving data protection statements attached to emails and other marketing copy
  - 2.8..2.Addressing data protection queries from clients, target audiences or media outlets
  - 2.8..3.Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy
- 2.9. The processing of all data must be: Necessary to deliver our services, in our legitimate interests and not unduly prejudice the individual's privacy and in most cases this provision will apply to routine business data processing activities.
- 2.10. Our Terms of Business contains a Privacy Notice relating to on data protection.
- The notice:
- Sets out the purposes for which we hold personal data on customers, employees, residents and service users
  - Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
  - Provides that service users and correspondents have a right of access to the personal data that we hold about them
- 2.11. 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.
- 2.12. 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.
- 2.13. 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 inform the DPO.
- 2.14. Reasonable steps must be taken to ensure that all personal data we hold is accurate and updated as required. For example, if personal circumstances change, please inform the Data Protection Officer so that they can update the records.
- 2.15. personal data must be kept secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.
- 2.16. In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- 2.17. Printed data should be shredded when it is no longer needed

- 2.18. 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.
- 2.19. Data stored on CDs or memory sticks must be locked away securely when they are not being used
- 2.20. The DPO must approve any cloud used to store data
- 2.21. Servers containing personal data must be kept in a secure location, away from general office space
- 2.22. Data should be regularly backed up in line with the council’s backup procedures
- 2.23. All servers containing sensitive data must be approved and protected by security software and strong firewall.
- 2.24. Personal data must be retained 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.
- 2.25. Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.
- 2.26. If you receive a subject access request, you should refer that request immediately to the DPO. Who may ask you to help us comply with those requests.
- 2.27. Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.
- 2.28. You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.
- 2.29. Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.
- 2.30. Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.
- 2.31. All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.
- 2.32. Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.
- 2.33. Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

<b>What information is being collected?</b>	
Who is collecting it?	

How is it collected?	
Why is it being collected?	
How will it be used?	
Who will it be shared with?	
Identity and contact details of any data controllers	
Retention period	

- 2.34. We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.
- 2.35. We will process personal data in compliance with all six data protection principles.
- 2.36. We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.
- 2.37. The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.
- 2.38. Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.
- 2.39. Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.
- 2.40. A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.
- 2.41. Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.
- 2.42. When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.
- 2.43. Regular data audits to manage and mitigate risks will inform 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.
- 2.44. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:
- 2.44..1. Investigate the failure and take remedial steps if necessary

- 2.44..2. Maintain a register of compliance failures
- 2.44..3. Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures
- 2.44..4. Please refer to our Compliance Failure Policy for our reporting procedure.
- 2.45. Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.
- 2.46. 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. A solicitor in breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.
- 2.47. If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Document History - DATA PROTECTION POLICY (AND INFORMATION SECURITY)		
Status	Date	Version
Draft to Clerk	28 <sup>th</sup> April 2018	1.0
Draft to Council for Debate	4 <sup>th</sup> May 2018	1.0
Council Approved	14 <sup>th</sup> May 2018	1.0
Next Review by Clerk		