MANLEY PARISH COUNCIL

Data Protection Act 2018 Policy

incorporating

General Data Protection Regulations (GDPR)

April 2022 – V1

Reviewed January 2024

This policy will be reviewed annually by the Parish Council members (or sooner if relevant changes are needed). Reviews will take place at the January meeting each year.

1. Policy Statement

This policy is to ensure that Manley Parish Council (**"MPC"**) fully endorses and adheres to the principles of the Data Protection Act 2018 ("**Regulations**") and the General Data Protection Regulations (**"GDPR"**).

These Regulations are designed to protect the use of individuals' personal data and provide them with rights to access their personal data held by organisations.

This policy, is designed to ensure compliance with the Regulations.

This policy may be updated from time-to-time, including when applicable laws or Regulations have changed.

2. Terms of the Regulations

Personal Data

Data relating to a living person who can be identified from it (either from that data alone or along with other information likely to come into the organisation's possession), such as name and address, including opinions about and indications of intention towards that person.

Data Subject

The person the data is about.

Data Controller

The person (legal or individual) who determines the purpose for which and the manner in which the data is processed. MPC's Information Commissioners Office (**"ICO"**) registration number is ZA186988.

Data Processor

Anyone processing the data on behalf of the data controller, other than the controller's employees.

Data Protection Officer

The MPC Chair handles all Data Protection issues and queries.

Sensitive Personal Data

Information on physical or mental health, sexual life, racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership or commission or alleged commission of any offences and proceedings. These types of data are all classed as sensitive personal data. This type of data is subject to further Regulations and can only be processed under certain circumstances – extra care must be taken!

Processing

In relation to data, Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including (amongst other things) altering the data, using the data, disclosing the data, or erasing/destroying the data.

3. What are the DPA/GDPR Regulations?

The Regulations provide a legal framework regulating the use of personal data in the UK. It was introduced to protect data subjects' privacy rights and freedoms "to promote high standards in handling of personal information and so to protect the individuals' right to privacy".

Data Protection Principles

There are 8 data protection principles. They state that personal data must be:

- Fairly and lawfully processed;
- Processed only for specified lawful purposes and not further processed in any manner incompatible with those purposes;
- Adequate, relevant and not excessive for those purposes;
- Accurate and up to date;
- Kept for no longer than necessary for those purposes;
- Processed in line with a data subject's rights under the Regulations;
- Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and accidental loss, destruction or damage; and
- Not transferred to a country outside the European Economic Area unless the rights and freedoms of the data subjects are adequately protected.

What Data is covered?

Any information which can be used to identify a living individual, whether on a computer, on paper, or in any other readable format and includes the following:

- Personal details, for example name, address;
- Reference numbers relating to an individual;
- Credit/Debit card numbers and details;
- Data on computer systems;
- Recorded phone calls;
- Emails; and
- Photographs and CCTV footage.

4. Transfer and Disclosure of Personal Data

MPC holds data for several purposes, such as - administration, advertising, reviewing tenders, minuting meetings and accepting and sending emails.

Councillors may only disclose the Personal Data of another person if at least one of the following apply:

- The disclosure is to that person or someone acting on their behalf;

- The person or the person acting on their behalf has requested or consented to the disclosure;
- The disclosure is required by law or by order of the court;
- The disclosure is required for the purpose of obtaining legal advice or in the course of legal proceedings;
- The disclosure is urgently needed to prevent injury or damage to the health of any person.

5. Data Subject Access Requests/Freedom of Information

Persons have the right to ask MPC to disclose what personal data is held about them. We have an obligation to reply to all such requests promptly and in any event within 30 calendar days of receipt. There is no charge for this service.

6. Personal Requests

The ICO Regulations also gives persons the right to receive information that is held on them. A person is entitled to:

- Ask for all the information held about them, wherever held and in whatever form (including computer records);
- Ask a data controller to stop processing where it is likely to cause substantial damage or distress to themselves or anyone else or is for direct marketing purposes;
- Apply to a court to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data;
- The request has to be made in writing; and
- These requests can be made by the person or by a 3rd party on their behalf. Either way, the request will only be processed upon receipt of written consent from the person.

Information Requests from Statutory Bodies

Requests from the Police; HM Customs or other Law Enforcement agencies, must be referred to the Chair.

7. Data Security

MPC must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
The Regulations require we have procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Maintaining data security means guaranteeing the confidentiality, integrity, and availability of the personal data, defined as follows:

- **Confidentiality**: Means that only individuals who are authorised to use the data can access it;
- **Integrity:** Means that the personal data should be accurate and suitable for the purposes for which it is processed; and
- **Availability:** Means that authorised users should be able to access the data if they need it for authorised purposes.

8. Data Protection Incidents

All breaches of the data protection rules must be reported to the Chair within 1 hour of occurrence. The Chair will keep a log of all breaches and take any further action required (i.e. any notifications to relevant Regulators and/or the data subjects).

9. Email Communications

As emails are not the most secure form of communication, we must be extra vigilant when communicating in this way. In particular, if personal data is sent via email for any reason, take particular care to ensure that the email is sent to the correct recipient (i.e. take care to ensure that personal data is not incorrectly disclosed to a third party).

10. MPC Obligations

MPC requires all Councillors to use their dedicated manleypc.co.uk email address and adhere to this policy as they play a key part in preventing data being passed to unauthorised parties.