Molescroft Parish Council

Information Management Policy

1. Policy Context

As a responsible corporate body Molescroft Parish Council (MPC) recognises and strives to work within a range of legislative frameworks relevant to managing personal and business data, namely the

- Data Protection Act 1998 (DPA)
- Freedom of Information Act 2000 (FOI)
- General Data Protection Regulations 2018 (GDPR)

In doing so, MPC recognises the benefits of proactive, planned and transparent practices in relation to information management and encourages good practice as normal practice across the Council.

MPC are committed to both protecting individual information rights and privacy under these frameworks whilst balancing the need to fulfil its duties, obligations and excise of powers inferred by the LGA 1972 as a corporate body.

In doing so, the legal bases described in the DPA 1998 regarding the lawful use, retention, sharing and destruction of information will be observed.

2. What this policy means for you and the Council

The suite of documents detailed below describes the Councils approach to managing information and constitutes the overall policy framework, this includes details of

- Information Risk Assessment & Action Plans (May 2018)
- Information held (Information Audit May 2018)
- Retention periods (Information Audit 2018)
- Information security and secure destruction methods
- Relevant behaviours and standards for information processing

All those involved in the discharge of duties will be expected to have read and work within this policy. This includes Councillors, paid staff and contractors working with or on behalf of MPC.

3. The lawful use of personal information – practicalities

In the course of discharging its duties, MPC collects and receives information for a variety of purposes (see Appendix A). Working within DPA frameworks, MPC will ensure personal information is:

Processed lawfully and in doing so the Council will state clearly what information is required and why. Indicating how long this information will be held for in the discharge of council duties.

Collected for specific purposes and in doing so the Council will only use the information for the purpose it was intended. If this data is requested by others outside of MPC then appropriate data sharing principles will be observed and information redacted to protect data subjects/third parties. Consent will be sought from data subjects where practicable in relation to historic data. Information gathered, recorded and stored after 25th May 2018 will be done so with the informed consent of the data subject.

Is adequate, relevant and limited to the purpose for which it is intended and in doing so the Council will monitor and review the information it holds and manage in accordance with retention schedules described at Appendix B.

Accurate and up to date and in doing so MPC will ensure annual information audits to enable sound data management in accordance with the stated retention periods at Appendix B.

Retained in a form and for a period no longer than necessary that will allow the identification of individuals (data subjects) and in doing so ensure review, retention and deletion schedules are observed. This will include a series of checks and balances by way of annual data audits.

Processed to ensure appropriate security of personal data including protection against unlawful processing. In doing so, MPC will endeavour to maintain appropriate technical and organisational measures, thus guarding against unlawful or unauthorised processing of personal data. This includes sharing with unauthorised third parties within and outside the UK.

4. Information Security – what this means in practice

When managing information and personal data especially that of others, information security **must** be considered.

In handling information, all Councillors, staff and contractors should consider

- What information is held/shared?
- How do I use this in the discharge of my role and duties?
- Do I need it?
- Where is information held and who else can access it?
- Have I made it secure?

In support of secure data handling, MPC will endeavour to provide secure storage of information hard and electronic. This includes (but is not limited to)

- lockable cupboards
- secure email
- GDPR compliant webhosting
- password protected computer equipment
- encrypted diskspace (subject to technical capability)
- hard copy information to be stored securely on site (Pavilion) where possible subject to operational needs
- confidential waste/destruction

Storage of personal subject access data on personal computers off site is not permitted unless agreed with the Clerk and all other provisions within this policy are fulfilled.

5. How we check what we do

Due diligence will be exercised by the Information Management Sub-Committee whose brief is to ensure this policy works well in practice. This includes

- An overview of data protection practices across MPC
- Record keeping and decision making in relation to all data protection matters
- Review of subject access queries
- Review of Freedom of Information queries
- Management of data breaches should they occur

In addition, this sub-committee working with the Clerk is responsible for liaison with the Information Commissioner should this be required on any data protection matter.

6. Want to know more?

Additional detailed information regarding data protection laws can be found at www.ico.gov.uk. This site provides the latest legislative updates and policy frameworks and clearly outlines rights and responsibilities in relation to data.

Alternatively, all enquiries relating to local policy and practice in MPC should be directed for the attention of the Clerk to the Council at clerk@molescroft-pc.gov.uk.

Policy Dated: 8th May 2018

Author: Eve Williams (Clerk to the Council)

Review Date: May 2021 or triggered by legislative change