

## Document Control Sheet

<b>Document title</b>	Data Protection Policy
<b>Summary of purpose</b>	To review and update the Council's Data Protection procedures in line with the requirements of the General Data Protection Regulations which come into force on 25 <sup>th</sup> May 2018.
<b>Prepared by</b>	Ian Phillipson
<b>Status</b>	Draft
<b>Version number</b>	2 (as amended by the Finance and Corporate Services Committee)
<b>Approved by</b>	F&CS – Full Council
<b>Approval date</b>	
<b>Date of implementation</b>	Immediate
<b>Review frequency</b>	3 years (Retention Schedule revised continuously to incorporate any changes/new documents)
<b>Next review date</b>	March 2021
<b>Circulation</b>	
<b>Published on the Council's website</b>	

## Validity Statement

This document is due for review by the date shown above, after which it may become invalid. Users of the strategy or policy should ensure that they are consulting the currently valid version of the document.

## **MALDON DISTRICT COUNCIL**

### **DATA PROTECTION POLICY**

Maldon District Council ('the Council') aims to ensure that personal information/data is treated lawfully and correctly.

The lawful and correct treatment of personal information is extremely important in maintaining the confidence of those with whom the Council deals and in achieving its objectives.

This policy applies to all officers, Members and those engaged undertaking business with or on behalf of the Council.

The Council fully endorses and adheres to the Data Protection principles set out below:-

### **DATA PROTECTION PRINCIPLES**

#### **Personal Information shall be:**

- Processed fairly, lawfully and in a transparent manner;
- Collected for specific, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to meet the purpose;
- Accurate and up to date;
- Kept for no longer than is necessary;
- Kept secure to maintain integrity and confidentiality;
- Processed in an accountable manner;

#### **Policy Aim**

To ensure the Council continuously complies with all relevant legislation and good practice in order to successfully protect the data it holds and processes.

#### **Policy Objectives**

To achieve the overall aim the Council will:

- Provide adequate resources to support an effective corporate approach to Data Protection;
- Ensure all staff are appropriately trained to perform their roles;
- Comply with all relevant statutory obligations;
- Respect the confidentiality of all personal data, irrespective of source;
- Publicise the Council's commitment to Data Protection;
- Compile and maintain appropriate policies, procedures and documentation;

- Promote general awareness and provide specific training, advice and guidance at all levels to ensure standards are met;
- Monitor and review compliance with legislation and introduce changes where necessary;
- Assist the Regulator and auditors as necessary

**Processing of Information:**

The Council, through appropriate management controls will, when processing personal information on any individual:

- Observe fully conditions regarding the collection and use of information meet the Council's legal obligations under Data Protection legislation;
- Collect, process and retain data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement;
- Ensure that the rights of people about whom information is held can be fully exercised including:-
  - The right to be informed that processing is being undertaken;
  - The right of access to personal information;
  - The right to withdraw or amend consent for processing\*;
  - The right to correct, amend or erase information\*;
  - The right to be forgotten\*.
- Ensure staff are reminded that data covered by Data Protection legislation is exempt from disclosure under the Freedom of Information Act 2000.
- \*Ensure where an individual exercises their right to be forgotten or withdraws permission for their data to be processed, the Council will inform the subject of the potential impact of this decision, as it may prevent the Council being able to provide a service which the subject has requested.
- **Note:** The right to be forgotten or withdraw permission for processing does not apply where there the Council has a statutory obligation or requirement to process that information.

**Fair Obtaining/Processing**

Individuals whose data is collected by the Council must be made aware at the time of collection of all the processes that data may be subject to. No manual or automatic processing of an individual's data can take place unless reasonable steps have been taken to make that individual aware of that processing.

Individuals must also be informed of likely recipients of their information, both internal and external, and also be given details of who to contact in order to query the use or content of their information (Data Protection Officer).

When consent is used as the lawful basis for processing data, it must be explicit and granular to allow the subject to 'opt-in' to any processing activity. The Privacy Notice where this data is collected should also explain how a subject's data will be used, how they can amend or withdraw their consent, and to whom they should contact to do so.

## **Data Uses and Purposes**

- All processing performed must only be for the purpose that is necessary to enable the Council to perform its duties and services, and which has been notified by the Council to the Information Commissioner. Personal data can only be processed in line with notified purposes.
- No new processing may take place UNTIL the Information Commissioner has been notified of the relevant purpose AND the data subjects have been informed and, their consent obtained. All new occurrences of, or future developments for, processing of personal data must therefore be reported to the Data Protection Officer, who is responsible for maintaining Council's Data Protection registrations.
- All personal data should be regarded as confidential and only disclosed to persons (internal and external) who are listed for the purpose concerned in the Council's current notification AND whose authority to receive it has been explicitly established.
- Information owned by the Council must not be used for non-Council purposes. This applies when Council data is being processed at employees' homes. Employees may only remove personal data from a Council office with the authority of their Chief Officer or the Chief Executive and will be held responsible for any misuse or unauthorised disclosures while the data is in their control.

## **What counts as Personal Data?**

The term 'personal data' applies to any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The regulations apply to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the regulations depending on how difficult it is to attribute the pseudonym to a particular individual. Likewise, anonymised data that can be 'reverse engineered', or manipulated on its own or in conjunction with other data sources to identify an individual, will also be classified as personal data.

A name and address, or information attached to a reference number that we can use to look someone up, are both personal data. So is a company e-mail address if it includes a person's name.

## **Data Quality**

Information processed shall not be excessive or irrelevant to the notified purposes.

Information will be held only for as long as is necessary for the notified purposes, after which it shall be deleted or destroyed in accordance with the Council's Document Retention Policy.

Whenever information is processed, reasonable measures shall be taken to ensure that it is up-to-date and accurate.

### **Organisational Responsibilities and Security**

All personal data should be kept secure, in a manner appropriate to its sensitivity and the likely harm should a breach occur. Security shall be applied to all stages of processing to prevent unauthorised access or disclosure (internal or external), damage (accidental or deliberate) or loss.

Personal data must not be left on display or unsecured when unattended. Computer software shall be kept secure when not in use. System entry passwords should be known only to the holder and be changed regularly.

Everyone managing and handling personal information is appropriately trained to do so.

Everyone managing and handling personal information is appropriately supervised.

Anybody wanting to make enquiries about handling personal information knows what to do.

Queries about handling personal information are promptly and courteously dealt with.

Methods of handling personal information are clearly described.

A regular review and audit is made of the way personal information is managed.

Methods of handling personal information are regularly assessed and evaluated.

Performance with handling personal information is regularly assessed and evaluated.

All Council employees and Members will be provided with a copy of the Policy as adopted by the Council together with appropriate training. Employees and Managers have a duty to follow the Policy and procedures and to co-operate with the Council to ensure this Policy is effective.

Action may be taken against any employee/Member who fails to comply or commits breach of the Policy.

It is the duty of individual employees and Members to ensure that personal information held by them is dealt with in accordance with the Data Protection legislation.

Processing carried out by a third party on behalf of the Council shall be subject to a contract, which stipulates compliance with Data Protection regulations and this policy.

Similarly, when the Council is processing personal data on behalf of a third party it will need to demonstrate that the data is subject to the same standards of care.

Any breaches of security shall be reported to the Data Protection Officer for investigation and subsequent remedial action.

### **Complaints & Queries**

Queries regarding this policy should be addressed to the Data Protection Officer:

[dpo@maldon.gov.uk](mailto:dpo@maldon.gov.uk)

If you are not happy with the Council's response to a Data Protection request you can complain using the Council's complaints system.

You can speak to your local Councillor(s) to see if they can resolve the issue for you.

If you are unclear who this is telephone the Council Officers 01621 875790 or visit our website [www.maldon.gov.uk](http://www.maldon.gov.uk)

You can complain to the Information Commissioner at:

Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Tel: 01625 545 700

Web: [www.ico.gov.uk](http://www.ico.gov.uk)

### **Large print and other versions of this guidance**

If you require a large print or Braille version of this leaflet or need it translated into another language, please ask at our reception at the Council Offices or telephone 01621 875790.