Mid Devon District Council

Data Protection Policy

Policy Number: IM 002

~~June 2019~~Aug 2022

Version Control Sheet

Title: **Data Protection Policy and Guidance**

Purpose: **To detail the commitment of MDDC to the protection of personal data, and to advise Officers, and Members, on the standards to be implemented regarding personal data processing.**

Owner: **Data Protection Officer** ~~Group Manager for Performance, Governance and Data Security cyandle~~gwallace@middevon.gov.uk
~~**01884 234975**~~

Version Number: **~~6~~5.0**

Status: ~~**Draft**~~**LIVE**

Review Frequency: ~~Every three years~~Triennial or before if new legislation is implemented.

Next review date: ~~**May 2022**~~**Aug 2025**

Consultation **This document was sent out for consultation to the following:**
Group Managers and Leadership Team

Document History
This document obtained the following approvals.

Title	Date	Version Approved
Data Protection Officer/Group Managers	July 2022~~18 June 2019~~	V6.0
Leadership Team	~~18 June 2019~~	V6.0
Cabinet	~~27 June 2019~~	V6.0

Roles

Senior Information Reporting Officer: Jill May

Data Protection Officer: ~~Catherine Yandle~~Giovanni Wallace

Group Managers; includes Head of Planning and Leisure Managers

Formatted: Font: Not Bold, Font color: Auto

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Data Protection Policy

1. Introduction

Mid Devon District Council (MDDC) is required to control and process personal data by virtue of its provision of services to the residents of the district and the legislative framework governing those services. This requirement to collect and process personal information is critical to the work carried out by Officers and Members.

Our residents, partners and suppliers have an expectation that they can deal with MDDC~~us~~ in the knowledge that the Council will process their data legally, transparently, without prejudice and only where necessary~~properly~~.

The Data Protection Act 2018 and the UK/GDPR provides the legislative framework and this policy provides the specific guidance for processing personal data within the Council.

2. Related Documents

Commented [GW1]: Will require additional policies to be entered here once written

ICT 0001 Information Security Policy
IM 001 Records Management Policy
ICT 0010 Freedom of Information Policy
ICT 0014 Information Security Incident Policy

3. Scope

This policy applies to everybody who has access to any personal data held by, or on behalf of, MDDC.

In order to operate efficiently, MDDC has to collect and use information about data subjects~~people~~ with whom it works and for whom it provides services. These may include members of the public, current, past and prospective employees, clients, customers, and suppliers.

In addition, the Council may be required to collect and process information in order to comply with specific legislative requirements.

The Data Protection Act and UK/GDPR requires that this personal information must be fairly and transparently collected and properly handled, ~~how ever~~however it is collected, recorded and used, ~~and~~ whether it be on paper, ~~in~~ computer files or recorded by any other means.

MDDC~~The Council~~ must ensure that all Employees, Elected Members, Contractors, Agents, Consultants, Partners or other servants of MDDC~~the Council~~ who have access to any personal data held by, or on behalf of MDDC~~the Council~~, are fully aware of and abide by their duties and responsibilities under the Act.

4. Policy Statement

MDDC~~The Council~~ regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between MDDC~~the Council~~ and those with whom it carries out business. ~~-~~MDDC~~The Council~~ will ensure that it treats personal information lawfully and correctly.
To this end MDDC~~the Council~~ fully endorses and adheres to the~~he six~~ Principles of Data Protection as set out in the Data Protection Act 2018 Data protection: The Data Protection Act - GOV.UK (www.gov.uk) and UK/GDPR The principles | ICO.

5. The principles of data protection

The Act stipulates that anyone processing personal data must comply with the ~~**Six**~~ **Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information shall be:

- **Lawfully, Fairly, Transparently** - Data will be processed lawfully, fairly and in a transparent manner in relation to individuals;
- **Purpose, Limitation** - Data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- **Data Minimisation** - Data collection will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **Accurate** – Collected Data will be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- **Storage Limitation** - Data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- **Integrity, Confidentiality** - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

~~1. processed lawfully, fairly and transparently in relation to the data subject;~~

- **Accountability** - The controller shall be responsible for, and be able to demonstrate compliance.

Formatted: Strong, Font: 11 pt
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font color: Auto
Formatted: Strong, Font: 11 pt
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font color: Auto
Formatted: Strong, Font: 11 pt
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font color: Auto
Formatted: Strong, Font: 11 pt
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font color: Auto
Formatted: Strong, Font: 11 pt
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font color: Auto
Formatted: Font: 12 pt
Formatted: Normal, No bullets or numbering
Formatted: Strong, Font: 11 pt
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font color: Auto
Formatted: Font: 12 pt
Formatted: Indent: Left: -0.63 cm, Bulleted + Level: 1 + Aligned at: 0.63 cm + Tab after: 1.27 cm + Indent at: 1.27 cm
Formatted: Strong, Font: 11 pt
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font color: Auto

6. Special Category Data

The DPA and UK/GDPR~~Act~~ provides conditions for the processing of any personal data. It also makes a distinction between **personal data and "special category" data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data or
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Special category data is defined as personal data consisting of information revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- ~~Processing of~~ Genetic data - for the purpose of uniquely identifying a natural person~~, or~~
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health;
- Sex life;
- Sexual orientation.

The aim of the policy is to ensure a legal framework for managing MDDC's processing of Personal Data and to ensure that the MDDC~~Council~~:

- creates and captures authentic and reliable records to demonstrate evidence, accountability and information about its decisions and activities
- facilitates auditing and protects its legal and other rights by;
  - maintaining personal records securely and preserving access to them
  - disposing appropriately of personal records that are no longer required
  - maintaining the accuracy of personal records
  - conforming to legal and statutory requirements relating to personal record keeping

6. Identification of roles and responsibilities

- The Senior Information Reporting Officer for MDDC is ultimately responsible for ensuring proper application of Data Protection within MDDC with the Data Protection Officer responsible for overseeing the day to day implementation of the Data Protection principles by Services in relation to personal data management as set out in this policy.
- The Data Protection Officer will provide the link between Leadership Team, Data Protection, Freedom of Information and Records Management practices. Where

Formatted: Font color: Auto

appropriate, this post will co-ordinate activities, such as maintaining the Publication Scheme.

- Group Managers are responsible for the management of personal data processed by their services, in accordance with this policy, and ensuring that all staff are aware of Data Protection requirements.
- All Councillors and Employees of MDDC will be responsible for ensuring that the personal data they control in relation to their work is maintained in accordance with the data protection principles.
- All Staff have the responsibility of ensuring compliance with the requirements of Data Protection legislation and this is included in their job descriptions

7. Training and Awareness

Since any MDDC employee may be involved in creating, maintaining and using personal information/records, it is vital that everyone understands their responsibilities as set out in this policy. All Officers and Councillors are required to have read and accepted the Data Protection Policy and in so doing agree to act in accordance with it and the data protection principles referred to above. This will be renewed annually. Group managers will ensure that staff responsible for managing personal data are appropriately trained or experienced and that all staff understand the need for proper management of personal data.

A mandatory training programme has been established to ensure that all staff are aware of their obligations concerning Data Protection, as well as Freedom of Information, Information Security Incidents and Information/Records Management.

8. Handling of personal/special category information

MDDC will apply, through this policy, appropriate management and the use of controls to:-

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information - only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply checks to determine the length of time information is held and ensure it is appropriately disposed of after use;
- Take appropriate technical and organisational security measures to safeguard personal information held;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

  These include:

Commented [GW2]: This requires the WfA and BYOD to be completed and then they will have to be cross referred at the lead of this policy.

- The right to be informed that processing is being undertaken;
- The right of access to their personal information within the statutory calendar month;
- The right to restrict or object to processing in certain circumstances;
- The right to rectify information found to be wrong;
- The right to erasure (also known as 'right to be forgotten');
- The right to data portability;
- Rights related to automated decision making and profiling.

In addition, MDDC~~the Council~~ will ensure that:

- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All Elected Members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/special category data are kept in a secure environment;
- Personal data held on computers, mobile devices and computer systems is protected by the use of secure passwords, as per the password policy ~~which have forced changes periodically~~;
- ~~Individual passwords should be such that they are not easily compromised.~~

All contractors, consultants, partners or other servants or agents of MDDC~~the Council~~ must:

- Ensure that they and all of their staff who have access to personal data held or processed for, or on behalf of MDDC~~the council~~, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between MDDC~~the Council~~ and that individual, company, partner or firm;
- Allow data protection audits by MDDC~~the Council~~ of data held on its behalf (if requested);
- ~~Indemnify~~Indemnify MDDC~~the Council~~ against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by MDDC~~the council~~ will be required to confirm that they will abide by the requirements of the DPA and UK/GDPR~~Act~~ with regard to information supplied by the MDDC~~Council~~.

9. Disclosure of Personal Data

Personal Data will only be disclosed in accordance with the provisions of the DPA or UK/GDPR

Any member of the public is entitled to request copies of all personal information that MDDC~~the Council~~ holds about them. This is called a Subject Access Request (SAR).

SAR forms should be completed by the person requesting their information and submitted to the Data Protection Officer, with proof of identification. Once the SAR form has been received the information should be provided within one calendar month.

Please note that where documents or files contain the personal information of several different people, this will be redacted in accordance with the DPA and UK/GDPR before releasing the information.

10. Violations of Rules and Procedures

- It is the responsibility of all employees to report any suspected data breach~~ of the DPA~~ or of this policy to their Group Manager using the Information Security Incident form at the end of that policy (ICT 00014) as soon as they become aware of it.
- It is the responsibility of all Members to report any suspected Data~~breach of the DPA~~, or this policy, to the Data Protection Officer as soon as they become aware of it.
- Disciplinary action in accordance with procedures approved by the Council may be taken against any employee or Member who deliberately breaches the DPA, UK/GDPR or the requirements of this policy. The Information Commissioner's Office may also investigate in this situation. Failure to comply by partners, agents or contractors may constitute a breach of their data sharing agreements or contracts.

11. Implementation

The Data Protection Officer has been appointed with overall responsibility for coordinating consistent Data protection implementation across the Council. Group Managers will be responsible for ensuring that the Policy is implemented within their services. Implementation will be led and monitored by the Data Protection Officer who will also have overall corporate responsibility for:

- The provision of cascade data protection training for staff within the Council.
- The development of best practice guidelines.
- Carrying out compliance checks or information audits to ensure adherence, with the Data Protection Act throughout the Council.

Formatted: Space Before: 0 pt, Tab stops: Not at 0.63 cm

12. Notification to the Information Commissioner

The DPA 2018 and UK/GDPR requires every data controller, who is processing personal data, to notify the Information Commissioner's Office, and to renew their notification on an annual basis. Any changes to the register must be notified to the Information Commissioner, within 28 days. Failure to notify is a criminal offence.

MDDC is registered and appears on the public register of data controllers maintained by the Information Commissioners Office.

The Data Protection Officer is responsible for notifying and updating the Information Commissioner's Office of changes to the processing of personal data by the Council.

Any changes made to the processing of personal data between annual notifications must be brought to the attention of the Data Protection Officer immediately.