Appendix 1

Mid Devon District Council

Data Protection Policy

Policy Number: IM 003

Aug 2025

Contents

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: **Head of Digital Transformation & Customer Engagement**
*Version Number: 7***.0**

Status: **Draft**

Review Frequency: **Triennial or before if new legislation is implemented**.

Next review date: **Aug 2028**

Consultation This document was sent out for consultation to the following:
IT & Information Governance (ITIG) Board

Document History

This document obtained the following approvals.

Title	**Date**	**Version Approved**
ITIG Board	Aug 2025	
Leadership Team	Aug 2025	
Cabinet	Sept 2025	

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 their personal data will be processed by MDDC in a way that is lawful, transparent, fair, without prejudice and only where necessary.

MDDC and MDDC electoral services are separate data controllers but are both subject to The Data Protection Act 2018 and the UK-GDPR. These provide the legislative framework. This policy provides specific guidance for processing personal data within the Council.

2. Relevant legislation

Data Use and Access Act 2025 (DUAA 2025)
Data Protection Act 2018 (DPA 2018)
Environmental Information Regulation 2004 (EIR)
Freedom of Information Act 2000 (FOI)
Privacy and Electronic Communication Regulation 2003 (PECR)
United Kingdom General Data Protection Regulations 2016 (UK GDPR)

3. Related Documents

IM 001 Information Security Policy IM
IM 004 Records Management Policy
IM 005 Freedom of Information Policy
IM 002 Information Security Incident Policy
IM 006 Data Quality Policy
IM 011 Artificial Intelligence Policy

4. Scope

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

To operate efficiently, MDDC must collect and use information about data subjects 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 to comply with specific legislative requirements.

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

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

5. Policy Statement

MDDC regards the lawful and correct treatment of personal information integral to the successful operations and to maintaining confidence between MDDC and those with whom it carries out business. MDDC will ensure that it treats personal information lawfully and correctly.

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

- Fully observe the 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 MDDC is complying with its obligations by design and default.
- 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 Data Protection legislation.

6. The principles of data protection

UK GDPR stipulates that organisations processing personal data must comply with 7 key principles which are legally enforceable and require that personal information shall be:

Processed lawfully, fairly, and transparently – Data will be processed in a manner that the individual would expect, a lawful basis for the processing has been identified and there is an accessible privacy notice that informs individuals how their personal data is collected, used, and protected.

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes **('purpose limitation'):** This means:

- Personal data will be used for the purpose it was intended for, and for a new purpose only if it is compatible with the original purpose. Compatible purposes are set out in Article 8A of the UK GDPR, and Schedule 5 to the DUAA 2025 and include scientific and historical research, archiving in the public interest, protecting public security, responding to an emergency crime, taxation, safeguarding, and legal obligation.

Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation')**
This means MDDC will collect the data necessary for our specified purposes, and no more than is sufficient to conduct these purposes.

- We will consider anonymisation and pseudonymisation where practical and will review the data we hold and delete information in line with our records management policy.

Accurate and, where necessary, kept up to date **('accuracy')**;

- MDDC must ensure that the personal data we hold is accurate and up to date. MDDC must take reasonable steps to keep data up to date and erase any data that is inaccurate or misleading subject to the nature of that data. Consideration must be taken of any challenges to the data.

Kept in a form which permits identification of data subjects and for no longer than is necessary **('storage limitation')**;

- MDDC holds data in accordance with statutory retention periods and organisational policy as set out in the Records Management Policy and Record Retention Schedules.

Personal data may be stored for longer periods as far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. These must be identified. In these circumstances consideration should be given as to whether data can be anonymised.
Processed in a manner that ensures appropriate security of the personal data **('integrity and confidentiality')**:

- All data is processed in line with information security and ICT Policies.
- Security procedures are implemented to ensure access control for the lifecycle of the data, including access control, secure file, use of encryption and secure methods of disposal.
- All users of personal data shall receive appropriate, timely and regular training.

The data controller shall be responsible for, and be able to demonstrate compliance **('accountability')**

- MDDC will ensure and identify through a clear decision-making process that its functions are conducted to ensure full compliance with the relevant legislation.

7. Processing of Personal Data

The DPA 2018 sets out the definition of personal data summarized below: 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.

We must only process this personal data if there is a valid lawful basis for processing. UK GDPR sets out seven lawful bases for processing.

- **Consent** – a person has given clear consent to process their data for one or more specific purposes.
- **Contract** – processing is necessary to perform a contract with a person or because they have asked for specific steps to be taken.
- **Legal obligation** – the processing is necessary to comply with the law.
- **Vital interests** – the processing is necessary to protect someone's life.
- **Public task** – the processing is necessary to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

8. Special Category Data

The DPA 2018 and UK GDPR identifies some personal data that requires extra protection because the use of this data could create significant risks to an individual's fundamental rights and freedoms. This is known as **"special category" data**.

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;
- Genetic data - for the purpose of uniquely identifying a natural person
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health;
- Sex life;
- Sexual orientation.

In addition to the requirement of one or more of the seven lawful bases to process special category personal data, the UK GDPR and the DPA 2018 set out additional conditions that must be met before this type of data can be processed.

Criminal Offence Data and Enforcement Processing

Article 10 of UK GDPR requires that criminal offence data (criminal allegations,

proceedings, or convictions) be also subject to special conditions when processing. Processing for non-law enforcement purposes requires a specific condition under the DPA 2018 Schedule 1 to be identified.

There are some limited circumstances where MDDC, acting as a competent authority, will process data for the purpose of criminal enforcement. In these circumstances UK-GDPR does not apply. Instead, a separate legislative framework contained in Part 3 of the DPA 2018 applies (Sections 29-81). These requirements should be complied with for any processing of this nature.

For any processing of special category or criminal offence data, the Council is required to have appropriate guidance that sets out how the Council meets its obligations under this part of the legislation. This is published on the MDDC website.

9. Right to be informed

Privacy Notices

It is MDDC's policy to be open and transparent about its processing of personal data and to ensure that information about the collection and use of personal data is available to people whose data is being processed. Information about what data is collected and how it is processed is published in privacy notices on the Council's website.

MDDC makes available privacy information to data subjects through our website and via digital forms or upon request.

We will regularly review the purposes for processing and when necessary, update the Privacy Notices.

10. Data Subject Rights and Requests

Personal data will only be disclosed in accordance with the provisions of the DPA 2018 or UK GDPR. Anyone is entitled to request copies of personal information that MDDC holds about them. This is called a Subject Access Request (SAR). Details of how data subject requests can be made are available on the MDDC website here. Data subjects will need proof of identification. MDDC will reserve the right to request clarification to aim to provide the specific data required by the requester.

Once the SAR form has been received and formal identification provided, the Information Managers will ensure that reasonable and proportionate searches are conducted to retrieve the requester's data.

The requester will have a right to the information we hold, subject to the exemptions in identified in the DPA 2018. This will include documents, letters, communications, and may include opinions that are related to the data subject. Information may be withheld subject to Schedule 1-5 either fully or partially with redactions.

MDDC will endeavor to respond to all SARs and other enquiries promptly and no later than one calendar month. If the request is substantial, we will reserve the right to extend to the full 90-day period as sanctioned in the DPA 2018. Data Subjects will be notified of this delay.

Additional requests will be considered separately. These include the following:

- Have inaccurate data amended or completed,
- Have personal data erased,
- Request the restriction of suppression of their personal data,
- Move, copy, or transfer personal data easily from one database to another or Organisation safely and securely without hindrance to usability,
- Object to the processing of their personal data in certain circumstances and their absolute right to stop their data being used for direct-marketing purposes,
- Object to profiling and other rights in relation to automated decision making.

11. Automated Decision Making and Artificial Intelligence

Automated decision making in processing is a rapidly evolving area of privacy. If a significant decision, defined as a decision that would produce a legal effect or similarly significant consequence on the data subject, is automated without any genuine or meaningful human involvement then Articles 22A to 22D of UK GDPR must be complied with. To this end MDDC will:

- Inform relevant data subjects of any automated decisions;
- Allow the customer to make representations;
- Offer the right to human intervention on request;
- Enable customers to contest any automated decision as defined in Article 22A

MDDC will keep a register of automated decision-making processes to ensure compliance with the provision in Article 22A-22D. For more details, please see IM 011 AI Policy.

12. Disclosure and Sharing of Personal Data

MDDC may share personal data we hold across council services in accordance with the privacy notices made available to data subjects, either at the point of initial contact or via our website.

We may also disclose personal data we hold to third parties, including:

- Contractors or suppliers (data processors) who work for us to deliver our services. A contract and/or a data processing agreement (DPA) must be in place with all data processors to be compliant with data protection legislation.
- Processors, including but not limited to, all contractors, consultants, partners or other servants or agents of MDDC must ensure that they and all of their staff who have access to personal data held or processed for, or on behalf of MDDC, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under data protection legislation. Any breach of any provision

of the legislation will be deemed as a breach of contract and handled accordingly.

- Any disclosure to another council or partner organisation will be made under an external data sharing agreement (DSA) or under specified parts of the data protection legislation, for example Schedule 2 DPA 2018.

13. Data Processing Requests

The DPA 2018 has provisions that allow public sector organisations to circumvent the principles laid down by UK GDPR in specific circumstances.
These will be received in the form of a Data Processing Request. These requests will be logged and reviewed by Information Management and upon assessing their validity and confirming the data in question, will respond. MDDC reserves the right not to comply with these requests as there is no requirement to comply. Provisions for this are provided in schedules 2-4 of the DPA 2018. Common examples would be crime and taxation and social care.

14. Data Protection Impact Assessments (DPIA)

Under Article 35 of UK GDPR it is a requirement that MDDC completes a risk assessment where processing operations are likely to result in a high risk to the rights and freedoms of individuals.

MDDC maintains a standard of privacy by design, by which all new policies, projects, services, and other changes will be developed with privacy and data protection as a key consideration. This will include completing a DPIA for all processing that is high risk, in accordance with the Data Protection Impact Assessment Policy.

A DPIA must be completed prior to any new, or changes to activities that involve the processing of personal data, to include: -.

- New Processing that involves personal data, which is considered high risk data,
- Use of new IT systems/applications for processing personal data,
- Large volumes of individuals data processed,
- Personal data of vulnerable individuals (adults/children),
- Processing highly sensitive personal data,
- Using AI technology to automate decision making and/or profiling,
- Use of CCTV.

The DPIA will be reviewed and authorised by the Senior Information Officer and the service area's Information Asset Owner in consultation with the Head of Digital Transformation and Customer Engagement and the Operations manager of ICT where necessary.

15. Data Breaches

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This can be either accidental or deliberate.

All staff and members have a duty to report a confirmed or suspected personal data breach via the internal reporting process as soon as they become aware using the Information Security Incident form found at the end of the Information Security Incident policy (IM 002)

16. Marketing and cookies

In addition to the requirements around Data Protection, there are additional provisions within PECR 2003, relating to Marketing and Use of Cookies. Marketing is communication of any kind that advertises to a customer. This can include any type of communication. MDDC will, in specific circumstances, market to their customers. While there is no requirement to comply with PECR when conducting their obligations as a public authority, some non-public processes, particularly around Leisure and other commercial activities, will need to comply with these provisions.

To this end MDDC will ensure we:

- Will only market to customers if we have either gained consent from the customer or have a clear legitimate interest to promote services or initiatives.
- Will ensure that customers are given clear opportunities to opt out of marketing at any time.

- MDDC may use cookies and tracking technologies to improve user experience.

Customers will have the right to withdraw consent, object to direct marketing and complain in accordance with the complaints provisions within this policy.

17. Information Commission Registration

The DPA 2018 and UK GDPR require data controllers who process personal data to register with the Information Commission, and to renew their registration on an annual basis. Any changes to the register must be notified to the Information Commission within 28 days. Failure to notify is a criminal offence.

MDDC and Electoral Services are registered and appear on the public register of data controllers maintained by the Information Commission.

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

18. 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 Members must 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.
Training will be renewed annually. operations 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. To this end MDDC will ensure all Officers handling personal data are appropriately trained and supervised.

19. R.A.C.I. Model

The RACI model is used for clarifying and defining roles and responsibilities in cross-functional or departmental projects and processes as detailed below:

- **Responsible**: All staff, members, or third-party providers of services or support who use MDDC assets and process data on behalf of MDDC.
- **Accountable:** SIRO, SRI, SIO acting as the DPO
- **Consult:** IT and Information Governance Board, with the Info.
- **Inform:** All staff, or third-party providers of services or support who process data for MDDC

20. Review of policy

This policy will be reviewed in 2028 or in accordance with any changes made to relevant legislation and to ensure the policy reflects any changes to formal guidance or local operational considerations.

Appendix 1 - Roles and Responsibilities

The **Senior Information Reporting Officer (SIRO)** for MDDC is responsible for ensuring proper application of Data Protection within MDDC – Deputy Chief Executive

The **IT and Information Governance Board (ITIG)** leads and advises on IT and Information Security. Any Data Protection reporting and related decisions will be discussed and made by this group. The ITIG board is accountable to the council through the portfolio holder, cabinet Member for Quality of Living, Equalities and Public Health, and The Leadership Team.

The **Senior Responsible Individual (SRI)** is responsible for monitoring compliance activities for Data Protection legislation, organising strategic and operational activities relating to data management, information security and training, and convening the ITIG – Head of Digital Transformation & Customer Engagement

The **Senior Information Officer (SIO)** acts as the Data Protection Officer and provides the operational link between senior leadership and the organization for Data Protection, Freedom of Information and Records Management practices. They will provide guidance, training and contribute to compliance activities. The SIO reports to the Head of Digital Transformation and Customer Engagement (SRI).

Information Management (IM) acts as the department that advises, processes, and ensures compliance with data protection and other associated areas. IM will develop and operate methods of handling personal information that are regularly assessed and evaluated;

Information Asset Owners 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. They act as the link between Information management and the other departments. These officers are Operational Managers and Service Leads.

All Members 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. To this end there is an expectation that officers will:

- Ensure paper files and other records or documents containing personal/special category data are kept in a secure environment. Ensure personal data held on computers, mobile devices and computer systems is protected using secure passwords and in accordance with MDDC Information and IT policies.