Data Protection Policy

1 Purpose

This Policy and accompanying procedures set out Metropolitan Thames Valley Housing's (MTVH) approach to processing personally identifiable data, including personal data, special category data and data relating to criminal offences.

2 Scope

This policy and any accompanying procedures apply to all MTVH colleagues, Board and Committee members, involved customers, consultants, contractors, and suppliers. It encompasses all entities within the MTVH group, and all business activities managed in partnership with other organisations. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3 Policy Statement

MTVH is committed to ensuring all personally identifiable data we process, including that of customers and colleagues is managed appropriately and in compliance with legislation. We will do this by following the data protection principles:

- Fair, lawful, and transparent
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

4 Our Approach

4.1 Roles and Responsibilities

Role	What are they responsible for:
Chief Executive	• Ensuring our compliance with legislation through this policy. MTVH also have a Senior Information Risk Owner (SIRO) who has oversight through the Data Steering Group.
Data Protection	• Monitoring compliance with this policy, • Advising the organisation on data protection matters • Ensuring data subject rights requests and personal data incidents are dealt with appropriately
Senior managers of all levels	• Ensuring that all systems, processes, records and datasets within their business area are compliant with this policy and with the legislation • Assisting the data protection department in their duties through providing all appropriate information and support, • Ensuring that their staff are aware of their data protection responsibilities • Consulting the data protection department on new developments or issues affecting the use of personal data in the organization • Ensuring that Data Protection Impact Assessments (DPIA's) and Legitimate Interests Assessments (LIA's) are completed where appropriate and that records of processing activities are completed for all processes where personal data is involved.

All colleagues	• Understanding and complying with relevant policies and procedures for handling personal data appropriate to their role • Immediately reporting any request, event or breach affecting personal data held by the organization

4.2 Data Protection by Design and Default

The legal requirement to practice data protection by design and by default must be considered before any decisions are made on processing or systems involving personal data.

To evidence the data protection by design and by default as well as to assess the risks of any new processing, we will complete ***Data Protection Impact Assessments (DPIA's)*** for all proposed new processing activities.

We have an obligation to implement technical and organisational measures to ensure the security of data throughout the organisation.

When introducing any new type of processing, particularly using new technologies, we will take into account whether the processing is likely to result in a high risk to the rights and freedoms of individuals and carry out DPIA.

4.3 Record of Processing Activity (ROPA)

A record of processing activity (ROPA) will be completed for all processes involving personal data. We will record our lawful basis for processing any personal, special category or criminal offence data, and particularly:

- Where we process personal data based on the consent of the data subject, we will have in place appropriate measures for documenting and managing that consent in line with the data subjects' rights. Where the data subject is a child, we will employ additional controls to further protect them.
- Where we process data based on legitimate interests, we will have in place a Legitimate Interests Assessment (LIA) that records the purpose, necessity and balancing tests which support this.
- Where special category or criminal offence data is processed, in addition to the above we will have in place a policy document as required by the legislation.

4.4 Data Sharing

In certain circumstances MTVH may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures or in unexpected or emergency situations.

Appropriate security measures will be used when sharing any personal data. Where data is shared regularly a contract, data protection addendum or data sharing agreement will be in place to establish what data will be shared and the agreed purpose.

MTVH will consider all the legal implications of sharing personal data prior to doing so. Data Subjects will be advised of any data sharing in the ***Privacy Notice***.

4.5 Monitoring and Compliance

The Data Protection Team along with internal auditors will carry out regular audits and compliance monitoring with a view to making sure the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times. Line managers will have oversight to act and perform spot checks if required.

4.6 Training

All colleagues will receive training, appropriate to their role, to help them understand how to process and handle data in line with the Policy and where to find guidance and support for data protection issues. They will complete the annual, mandatory data protection and information security awareness training and other training as and when required. Refer to the ***Learning and Development Programme.***

All line managers will be responsible for checking completion of colleague training within the Learning and Development system.

5 Legal/Regulatory Context

The overriding laws which govern the use of personal data are:

- Data Protection Act 2018 (including the Applied UK GDPR)
- UK General Data Protection Regulation (UK GDPR)

In addition, there is legislation, which is not specific to data protection, but must be considered and includes but is not limited to:

- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003

Related procedures and guidance:

- Data Breach
- Information Rights Request – formerly Subject Access Request (SAR)
- Information Sharing and Consent to Share Procedure
- New Processing of Data - including Data Processing Agreement, Data Protection Impact Assessment (DPIA), Legitimate Interests Assessment (LIA), Record of Processing Activities (ROPA) Template
- Further guidance can also be found on the Information Commissioners Office website at ico.org.uk.

6 Our commitment to Equality, Diversity and Inclusion

In implementing this policy MTVH will not discriminate against any colleague, customer or stakeholder on the grounds of their gender, sexual orientation, gender reassignment status, ethnic origin, age, religious belief, disability, marital status and pregnancy/maternity.

7 Key Policy Information

Policy Owner	Chief Information Officer
Author	Data Protection - ICT
Approved by	Data Steering Group
Effective from	December 2021
Approach to review	This Policy & associated Procedures will be reviewed every 3 years or sooner if legislation, regulatory changes or operational need require an earlier review. Any amendments will be appropriately consulted on and signed off before being clearly communicated to customers and colleagues.