Policy title	**Data Protection Policy**
Summary	This Policy sets out how MSV Housing will fulfill its obligations under the UK General Data Protection Regulations (UK GDPR) and Data Protection Act (2018).
Scope	The policy applies to all employees and Board/Committee members.
Author & Job Role	Kieran Hill – Data Protection and Assurance Officer
Directorate	Finance
Document Status	FINAL
Document Reference	CEX/SE/PO/3.0
Dates: - **Draft** - **Approved** - **Ratified** - **Effective from** - **Review by**	 November 2025 Audit & Risk Committee January 2026 N/A January 2026 December 27
Impact Assessments: **Date EIA completed** **Date other IAs completed**	December 2025 n/a
Consultation	GDPR Steering Group, Senior Leadership Team, Executive Leadership Team.

If you are reading a printed version of this document, you should check the intranet to ensure you are using the most up to date version of this Policy.

Contents Page

1. Introduction & Policy Purpose

1.1 In carrying out its day-to-day business and duties MSV Housing ("the Group") needs to collect and use certain information about individuals. This can include customers, employees, board members, suppliers, business contacts and other third parties the Group has a relationship with.

1.2 The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) place various duties and responsibilities on the Group when processing information. The UK GDPR and DPA also create legal rights for individuals in respect of personal information held and processed.

1.3 The purpose of this policy is to:

- set out MSV's overarching approach to ensuring compliance with the data protection legislation and regulations.
- provide information to employees on their obligations in relation to data protection.
- outline the rights of data subjects in relation to personal data.

2 Scope

2.1 This policy applies to all parts of MSV and to all personal data held and processed by the Group, or on behalf of the Group. This includes data held in any system or format, whether electronic or hard copy and whether it relates to potential, present or past data subjects.

2.2 It applies to all employees, temporary workers, consultants, contractors, volunteers and any other third parties who have access to personal data. They must be aware of and are required to comply with this data protection policy and associated procedures. This policy also applies where MSV is a joint controller or where it acts as a processor for another controller.

3. Key Legal Requirements

3.1 The UK GDPR outlines six principles of data processing, specific legal bases for processing personal data and special categories of personal data as well as specific rights for data subjects and certain exemptions.

3.2 Anyone processing personal data on MSV Housing's behalf is expected to comply with these requirements which are summarised overleaf:

a) Principles:

The Group will:

- process personal data in a lawful, fair and transparent manner (*lawfulness, fairness and transparency*').
- only process personal data for specific, explicit and legitimate purposes, which it will document (*purpose limitation*').
- only process data that is adequate, relevant and limited to what is necessary for the purposes for which they are processed (*data minimisation*').
- ensure all data processed is accurate and up to date to the best of its ability(*accuracy*').
- not keeping personal data for longer than it is necessary for the purposes for which it is processed (*storage limitation/retention'*).
- process data in a secure manner ensuring protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technological or organisational measures (*integrity and confidentiality/security*').
- remain accountable for processing personal data and ensure compliance with the above principles (*accountability*).

b) Specific Legal Rights

Before any processing activity takes place, MSV Housing will establish the appropriate lawful basis for such processing, which must be one of the following:

- The Data Subject has given consent to the processing of their data: or
- The processing is necessary for a contract the Data Subject is party to, or in order to take steps prior to entering into a contract (e.g. a Tenancy Agreement, or applying for a tenancy); or
- The processing is necessary for compliance with a legal obligation to which the Group is subject, or
- The processing is necessary to protect the vital interests (life) of the data subject or another natural person (e.g. in an emergency life and death situation, disclosing an employee's allergies); or
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- The processing is necessary for the purposes of a legitimate interest of the Data Controller or by a third party except where such interests are overridden by the interests or rights and freedoms of the Data Subject, in particular where the Data Subject is a child.

c) Rights for data subjects:

The Group will ensure it complies with the following rights:

- *The right to be informed* about the processing of their personal data.
- *The right to access* a copy of their data (Subject Access Request) MSV will respond to requests for personal data within one calendar month (extendable by a further 2 months as detailed in the separate Subject Access Procedure)
- *The right to rectification* if their data is incorrect.

- *The right to erasure* (also known as 'the right to be forgotten')
- *The right to the restriction of processing*
- *The right to data portability* to allow individuals to obtain and reuse their personal data for their own purposes across different services.
- *The right to object* to processing in certain circumstances.
- *Rights in relation to automated decision making and profiling*; where the automated decision could have a significant impact on them, and the associated right to request that a human reviews the decision made electronically.

d) Sharing Personal Data

Any data sharing and disclosure the Group undertakes will comply with our legal obligations and follow MSV's procedures to ensure the appropriate checks and verification are carried out.

When MSV engages in regular sharing arrangements with a third party, both parties will be required to sign and retain a Data Processing Agreement.

MSV will ensure that when appointing new suppliers/ partners, an assessment of data sharing and data processing will be completed and documented.

e) Transferring Personal Data outside of the UK

Wherever possible, all data processed on behalf of the Group will be held and managed withing the UK. If, due to certain circumstances, data must be processed outside of the UK then MSV will ensure compliance with the relevant requirements of the legislation.

f) Exemptions

There are certain exemptions within the UK GDPR which mean that in very special circumstances MSV does not have to comply with the principles, or with the data subjects' rights. These exemptions include, but are not restricted to:

- Prevention, detection or prosecution of criminal offences.
- Taxation, public health or social security purposes.
- Protection of judicial independence and judicial proceedings.
- Matters of public security, national security or defence.
- Safeguarding children or individuals at risk.

3.3 The Group has several procedures in place which set out how it complies with the legal requirements covered within this section. These are listed on the Heart under the GDPR section or available from DataProtection@msvhousing.co.uk

4. Lawful Processing

4.1 Record of Processing Activities (ROPA)

MSV will keep a record of processing activities (ROPA). This includes the reason and legal basis for processing of personal data.

This ROPA will be updated annually, or when there is significant change to processing. This includes either a new activity that requires data to be processed or a change in the legal basis for processing data.

4.2 Data Breaches

MSV's Data Protection Officer (DPO) will investigate all suspected and identified data breaches and assess the requirement to report to the Information Commissioner's Office (ICO) within 72 hours of the incident having been identified within the business.

The DPO will duly notify the ICO of any personal data breach considered to meet the ICO reporting thresholds within the 72-hour reporting deadline. The rationale for the basis for reporting to and not reporting to the ICO will be retained.

Staff will be supported to identify and report suspected breaches via training.

MSV will ensure there is a published procedure outlining the actions required in the event of a suspected data breach.

4.3 Marketing and Electronic Communications

MSV will ensure that it is compliant with the Privacy and Electronic Communications Regulations (PECR). This covers:

- Marketing by electronic means, including marketing calls, texts and emails.
- The use of cookies or similar technologies that track information about people accessing a website or other electronic service.
- Security of public electronic communications services.
- Privacy of customers using communications networks or services regarding traffic and location data, itemised billing, line identification services and directory listings.

5. Data Protection Complaints

5.1 MSV takes any concerns with regard an individual's data rights seriously. Data protection concerns will be managed outside MSV's standard complaints process and procedure. Any complaint relating to the handling of personal data will be managed in line with the ICO's recommended approach for managing and responding to data protection complaints.

5.2 MSV will comply with the requirements of the Digital Use and Access Act 2025 (DUAA) when processing data protection related queries and complaints, including acknowledging complaints within 30 days and responding to them 'without undue delay'.

5.3 MSV will ensure there is a published Data Protection Complaints Procedure.

6. Definitions

Data Protection Terms	Definition
Personal Data	Any information relating to a living, identified, or identifiable individual, e.g., on a computer, CCTV, backed up files, videos, emails, information on telephone logging systems, photographs, text/WhatsApp messages. An identifiable individual is one who can be identified, directly or indirectly by reference to: • A name, photo, job title, email address. • An identification number like an employee number. • Location data such as a home address or tracing location of a mobile phone. • An online identifier via IP address, internet cookies, social media account.
Data Subject	The identified or identifiable individual whose personal data is held or processed. For MSV this includes past, present and prospective: • Employees • Board/Committee Members • Customers, Service Users, Leaseholders • Contractors, Partners and Agents • Suppliers
Special Categories of Personal Data	Personal data, which is more sensitive and so needs more protection, including information about an individual: • Racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trade union membership. • Processing or genetic data. • Biometric data for uniquely identifying an individual. • Data concerning health. • Data concerning an individual's sex life or sexual orientation
Data Controller	A person or organisation that determines (either alone or jointly) whose personal data is held or processed and determines the purposes and means of the processing of personal data.
Data Processor	A person or other body, other than the employee of the data controller, who processes personal data on behalf of the data controller.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data Protection Terms	Definition
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, Loss, alteration unauthorised disclosure of, or access to personal data.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Senior Information Risk Owner (SIRO)	A nominated senior professional who has responsibility for implementing and managing data protection risks withing the organisation.

7. Roles and Responsibilities

a) The Audit & Risk Committee (ARC) is responsible for:

- Obtaining assurances relating to the adequacy and effectiveness of risk, control and governance relating to the data protection framework at MSV.

b) The Head of Risk and Assurance, acting as the Senior Information Risk Officer (SIRO) is responsible for:

- Having overall responsibility for the data protection framework.
- Appointing the Data Protection Officer (DPO) and seeking advice from them as appropriate.
- Ensuring registrations with the ICO are accurate and up to date.
- Acting as the key contact for the ICO.
- Establishing and overseeing the data protection framework.
- Ensuring the review of the MSV's Data Protection Policy and supporting procedures on a regular basis.
- Reporting regularly to the Executive Team and the Audit & Risk Committee on data protection compliance.
- Arranging data protection training and advice for all staff members and those included in this policy.
- Providing guidance and advice to colleagues on data protection matters.

c) The Data Protection Officer is responsible for:

- Advising MSV about their obligations to comply with UK GDPR and other data protection legislation.
- Advising, monitoring and assessing the Group's compliance with data protection legislation and making improvement recommendations.
- Providing guidance and advice on data protection to Board/Committee members, employees and other stakeholders.
- Advising on and updating data protection policies and procedures.
- Overseeing the Breach and Subject Access Requests (SAR) registers.

- Investigating suspected and identified data breaches and reporting to the ICO, where required.
- Carrying out data protection audits if required.
- Having a direct route of access to the CEO or Chair of ARC or Board, if they deem necessary.

d) The GDPR Steering Group is responsible for:

- Overseeing, monitoring and maintaining the data protection framework to ensure good practice.
- Ensuring compliance with MSV's policy and related procedures and reviewing these on a regular basis.
- Contributing to the development and improvement of the data protection framework.
- Identifying and managing data protection risks.
- Championing and promoting excellent data protection standards.
- Providing guidance and advice to colleagues on data protection matters.

e) The Director – ICT and Business Improvement is responsible for:

- Ensuring all IT systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.

f) Leaders are responsible for:

- Ensuring that all colleagues in their teams understand this Data Protection Policy and related procedures.
- Ensuring team members complete relevant data protection training.
- Assisting with the implementation of the requirements of UK GDPR and compliance.
- Developing policies and procedures with reference to the data protection principles.
- Raising queries and concerns with the DPO in a timely manner to enable matters to be investigated and resolved.
- Encouraging the reporting of data protection incidents as part of continuously improving standards of data protection.
- Support their team members with any queries.

g) Employees are responsible for:

- Complying with this Data Protection Policy and related procedures.
- Attending and completing all mandatory data protection training.
- Fully understanding their data protection obligations.
- Reporting any suspected data protection incidents.
- Asking for advice or guidance if they are unsure of any data protection practice.
- Checking that any data processing activities they are dealing with comply with MSV's policy and are justified and lawful.

- Raising any concerns, notifying any breaches or errors, and reporting anything suspicious or contradictory to this policy or our legal obligations to their line manager, DPO or a member of the GDPR Steering Group.

6. Monitoring, Review & Evaluation

The effectiveness of this policy will be monitored by:

- Regular reporting to the Executive Team and ARC
- Regular review by the GDPR Steering Group and DPO.

7. Policy Review

We will review this Policy every three years and upon changes to the Group. More regular reviews will be considered where, for example, there is a need to respond to new legislation / policy guidance. Reviews will consider legislative, performance standard and good practice changes.

8. Related Documents

- Records Management Policy
- Record of Processing Activity
- Retention Policy & Schedule
- Information Security Policy
- Data Breach Procedure
- Subject Access Request Procedure
- Data Protection Complaints Procedure
- DPIA Procedure
- Privacy Statements
- ICT Security Policy
- Social Media Policy
- Business Continuity Plans

9. Version History

Version	Date	Description/ Summary	Status	Author
0.1	11/22	First Draft	Final	HSE
0.2	12/23	2nd final version	Final	SL
0.3	11/25	3rd final version	Final	KH

EQUALITY IMPACT ASSESSMENT (EIA) – Data Protection Policy

Name of Strategy/Policy	Data Protection Policy
Date of Assessment	4 December 2025
Name & Role of Assessors	Alison Riley – Head of Risk and Assurance Joanne Tedds – EDI Lead
What are the desired outcomes of the policy?	To ensure MSV remains compliance with Data Protection laws and regulation.
Who are the main stakeholders in relation to the function?	MSV management, Board, customers, colleagues and 3rd parties including suppliers and partners
Who will be consulted and what types of consultation will be carried out?	Senior Leadership Team, Executive Leadership Team and Audit and Risk Committee. Consultation will be via presentation of the proposed policy and discussion of current management arrangements.
Summarise any evidence considered	Detailed EQIA completed on the draft SAR procedure in partnership with the MSV EDI Lead has confirmed that supporting procedures will be EQIA'd and identify any detailed considerations as we continue to improve the data protection framework.

Could the function have a differential impact on:		**What evidence exists to support your analysis?**
General Comments	**Yes / No**	
Race Consider language and cultural factors	No	In itself no. The data protection framework will be supported with a range of procedures. These detailed procedures will be EQIA'd and any mitigations identified will be actioned. The EQIA of the SAR procedure has identified the value of completing demographic analysis (approx. 200 cases per year) In addition, the additional requirements when processing special category data which includes racial and ethnic origin are documented in the Record of Processing Activity (RoPA)
Gender reassignment Consider people proposing to or have undergone a process of having their sex reassigned.	No	The additional requirements when processing special category data which includes data concerning sex life and sexual orientation are documented in the Record od Processing Activity (RoPA)
Disability Consider physical, visual, aural impairment, mental, learning difficulties	No	The additional requirements when processing special category data which includes data concerning health are documented in the Record of Processing Activity (RoPA)
Age Consider Elderly or young people	No	Considerations with regard age will be considered in the individual procedure EQIA's.
Sexuality	No	The additional requirements when processing

Either know or perceived		special category data which includes data concerning sex life and sexual orientation are documented in the Record od Processing Activity (RoPA)
Gender	No	Considerations with regard gender will be considered in the individual procedure EQIA's.
Religion or belief Consider religious or cultural observance including non-belief, practices of worship	No	The additional requirements when processing special category data which includes religion and beliefs are documented in the Record of Processing Activity (RoPA)
Other protected or vulnerable characteristics: • marriage or civil partnerships • pregnancy or maternity?	No	Political opinions and trade union membership are also considered special category data and therefore have additional requirements when processing.

If the answer is NO to <u>all</u> questions and no differential treatment has been found there is no requirement for a full Equality Impact Assessment. Please go back regularly and review the cycle.
If the answer is YES to any of the questions, please complete the rest of the form.

In what areas could the differential identified be considered to have an adverse impact in this function and what solutions will be introduced to overcome these adverse impacts?	N/A
In what areas could the differential identified be considered a positive impact in this function and what strategies will be introduced to safeguard and spread these positive impacts?	N/A
Which Action Plans have these solutions/strategies been transferred into?	N/A
Who will be responsible for monitoring these Action Plans?	N/A

Ratified by: Audit and Risk Committee **Date: 27 January 2026**
(Highlight as appropriate)