Data Protection Policy and Procedure

Version Control						
Version	**Date drafted**	**Date approved**	**Approved by**	**Date reviewed**	**Next review date**	**Owner**
Final v1	20/09/2020	12/10/2020	Board	N/A	12/10/2023	Chief Executive
2023 review				23/10/2023	23/10/2026	Data Protection Officer

1. Introduction

1.1. Westmoreland Supported Housing Limited (WSHL) is committed to respecting the privacy and information rights of individuals and processing personal data in accordance the Data Protection Act 2018 (the Act) and the UK General Data Protection Regulation (GDPR). The Information Commissioner's Office (ICO) is the supervisory authority for data protection in the UK: it issues guidance on data protection and we will follow this guidance.

1.2. As part of our work we are required to collect and use certain types of information about individuals who come into contact with our organisation. This personal information must be handled properly irrespective of how it is collected, recorded and used – whether on paper, on a computer, or recorded on other material.

1.3. This policy sets out responsibilities and our practices for complying with the law including our responsibilities about the collection, use and disclosure of data and customer's rights to access their personal data.

2. Legal and Regulatory Responsibilities (not exhaustive)

- The Data Protection Act 2018 (which brings the GDPR into UK law)
- UK General Data Protection Regulations (GDPR)

3. Scope

3.1. This policy covers all our business activity including:

- Tenants and applicants for housing
- Employees and applicants for employment
- Board and committee members
- Clients and grant recipients
- Contractors, external agents, support providers and consultants

4. Definitions

4.1. **Data controller** is the person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed.

4.2. **Data subjects** are individuals for whom personal data is collected; we call them individuals in this policy.

4.3. **Lawful basis** is the basis on which data can be processed as described in the GDPR. There are 6 available lawful bases as follows:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

4.4. **Personal data** is information that identifies a living individual either by that data alone, or in conjunction with other data held.

4.5. **Processor** is someone who is responsible for processing personal data on behalf of the controller.

4.6. **Special category data** is data that needs more protection because it is sensitive.

5. Policy Principles

5.1. We take data protection seriously and are committed to handling the personal information we hold sensitively, appropriately and legally. We fully adhere to the Principles of Data Protection, as detailed in the Act:

i. **Lawfulness, fairness and transparency** – data collection must be fair, for a legal purpose and we must be open and transparent about how the data will be used
ii. **Purpose limitation** – data is collected for specific, explicit and legitimate purpose
iii. **Data minimisation** – data is adequate, relevant and limited to what is necessary
iv. **Accuracy** – data is accurate and where necessary data is kept up to date
v. **Storage limitation** – data is not kept for longer than is necessary
vi. **Integrity and confidentiality** – appropriate security of personal data
vii. **Accountability** – taking responsibility for what we do with personal data, having measures in place that show that we comply with the law

5.2. All customers will be made aware of their rights. Board Members, employees and potential employees will be made aware of their responsibilities under the Act and the rights of our customers and individuals using our services. They will be required to lead by example in demonstrating good conduct and ensuring compliance with legal requirements, rules, and procedures.

5.3. We will make sure our partners also understand our stance and their obligations by publishing this policy and (where appropriate) by including clauses in our contracts to make this clear.

6. Collecting and Processing of Personal Data

6.1. We will provide privacy information to individuals when we collect data from them. When we obtain personal data for the first time and when any new data is collected, we will explain:

- Why the personal data is required and held
- The purposes for which the data may be used
- Who may have access to the data

6.2. We will ensure personal data we collect, and process is:

- **Adequate** – sufficient to meet our purpose
- **Relevant** – has a link to our purpose
- **Limited to what is necessary** – we will not hold more than we need

6.3. We will ensure that the "lawful basis" for collecting and processing personal information is identified and recorded.

6.4. As a provider of supported housing we need to collect and hold more sensitive personal data (described as "special category" information within the Act) to provide our services, to help customers access care services they need or to deal with neighbour disputes. We will always seek clear consent for this and explain why we need it and who we will share the information with, see also our privacy statement. We have stricter access requirements to this information within WSHL.

6.5. We will take reasonable steps to ensure that personal data is kept up to date and to encourage individuals to let us know of any changes. We cannot be held responsible for any errors or inaccuracies in personal data being held and processed where we have not been provided with up-to-date information.

7. Security of Personal Data

7.1. We are committed to retaining personal data securely in whatever format it is stored. We recognise and respect an individuals' rights to privacy and their expectation that personal data will be handled sensitively and in accordance with the law.

7.2. We will take appropriate steps to keep our computer systems secure and to protect personal data from unauthorised access, disclosure and/or loss. This includes:

- Firewalls and internet gateway
- Secure configuration of hardware and software
- Access controls
- Anti-virus and anti-malware software
- Backing up data regularly
- Using secure arrangements when transferring data
- Monitor security messages from software and access control logs
- Training staff in safe use of IT and protecting data

7.3. We will give staff and, where relevant, Board Members advice on the necessary physical security arrangements to be adopted appropriate to the level of confidentiality required for the personal data concerned. We will also provide guidance on keeping data secure and for dealing with disclosure requests.

7.4. Where other organisations are contracted to carry out work on our behalf, we will make expectations clear on their role in protecting personal data, such as tenant contact details provided to repairs and maintenance contractors.

7.5. Where we will be carrying out a project that involves the processing of personal data and where there is a high risk to individuals, we will carry out a Data Protection Impact Assessment in line with ICO guidelines.

8. Data Breaches

8.1. All staff and Board Members are required to report any data security breaches or suspected breaches, relating to unauthorised access to or disclosure of personal data, immediately using the data breach procedure.

8.2. We will take all reasonable steps to ensure that any organisation with whom we share data notifies us of any data breach, where this relates to or may relate to personal data which we have shared with them.

8.3. All data breaches will be taken seriously, will be investigated and lessons learned will be shared to reduce the chances of a future breach. Data breaches may be reported to the ICO where required to do so as set out in their data breach guidance.

9. Disclosure of Information and Data Sharing

9.1. We do not share data with colleagues or others that it is not necessary or relevant for them to hold to carry out their work. However, in order for us to operate effectively there will be some instances when personal data will need to be disclosed and/or discussed with other appropriate colleagues or individuals. In such instances this disclosure, whether it is written or verbal, will be appropriate and reasonable for business purposes, on a need-to-know basis only and in line with data protection legislation and, where possible, in accordance with ICO guidance.

9.2. Personal data relating to individuals will be considered confidential and will only be passed to other organisations with the express written consent of the individual concerned unless they are directly related to our responsibilities and legitimate interests as a landlord (e.g. tenant contact details provided to enable a contractor to carry out repairs or improvement works or to obtain customer views on our services) or where there are exceptional circumstances, see below. Where we seek consent to share data we will explain why and to whom that data may be disclosed.

9.3. However, in some circumstances and in order for us to provide our services more effectively we may enter into information sharing protocols with other organisations. All data sharing protocols will be reviewed regularly to ensure that they remain relevant and up to date.

9.4. Only in exceptional circumstances will we share personal data about an individual without their consent. Such exceptional circumstances include the following:

- Where the health and safety of an individual may be at risk if the information was not shared
- Where it is needed to carry out our duties as a landlord
- In connection with legal proceedings
- To comply with the law
- Where there is clear evidence of fraud

10. Retaining and Disposing of Data

10.1. All personal data that is held will be relevant for the purpose for which it is required and will be kept securely. It will be retained for the period set out in our Records Retention Policy, and for no longer except where a contract requires otherwise.

10.2. We will regularly review data we hold and erase or anonymise it to comply with our document retention guidelines. Where personal data is no longer required, it will be destroyed in a secure manner.

11. Access to Information

11.1. Individuals may request a copy of information held about them by us (data subject access request) and can seek to have it amended or erased if it is inaccurate or no longer required. An individual is entitled to ask for confirmation that we are processing their data and ask for a copy of it together with supplementary information. An individual is not entitled to information relating to other people (unless their data also relates to other individuals).

11.2. We will respond to any subject access requests as quickly as possible, but within the required period, i.e. within one month of receipt of the request.

11.3. Where it is not possible to complete a request the individual will be informed in writing, with a full explanation. We will follow ICO guidance in meeting requests, circumstances where a request may not be met include the following:

- Where the request is manifestly unfounded
- Where the request is excessive
- Where the request would mean disclosing information about another individual who has not given their consent and it would not be reasonable to disclose

11.4. Individuals have the right to request inaccurate data be rectified or completed if it is incomplete. We will make any changes within one month of receipt of the request or in line with the ICO guidelines. If we are satisfied that our data is accurate, we may not comply with a request or there may be other reasons we cannot comply. We would explain these clearly to the individual.

11.5. In certain circumstances individuals also have the following rights and we will ensure appropriate arrangements are put in place to exercise these:

- **Right to erasure** – right to have personal data erased
- **Right to restrict processing** – right to restrict or suppress personal data
- **Right to data portability** – right to obtain and reuse personal data for their own purposes
- **Right to object** – right to object to their data being used in certain circumstances
- **Rights related to automated decision making** – we do not use automated decision making

11.6. Individuals have the right to receive a copy of information held about them free of charge. However, we reserve the right to make a reasonable charge for responding to requests which are excessive or repetitive.

12. Raising Concerns

12.1. Board Members, employees, our customers and the general public are an important part of our compliance with the principles of data protection. They are encouraged to raise any concerns they may have in respect of data protection. A number of different channels for communication are available, including via senior officers, auditors, Board Members and via the Whistleblowing Policy. Our customers and members of the public may also use our complaints procedure for this purpose where appropriate. All allegations of data breaches, or poor data practice, will be investigated.

13. Responsibilities

13.1. WSHL's Data Protection Officer (DPO) has overall responsibility for Data Protection within WSHL, and for ensuring that we comply with ICO requirements including documentation and payment of the data protection fee.

13.2. The responsibility for data protection is shared by all WSHL staff. Each senior manager will have responsibility for their area of operation. They are encouraged to raise any concerns if breach of the policy is suspected.

13.3. Line managers are responsible for ensuring newly appointed employees are aware of this policy and their responsibilities relating to their role.

14. Monitoring and Review

14.1. WSHL will carry out audits and review the personal data we collect and update our records accordingly.

14.2. We will record data access requests and monitor responses.

14.3. We will investigate all concerns raised and reports of any data breaches, record the outcome of these investigations and lessons learned. The outcomes will be reported to the Board.

14.4. This policy will be reviewed every three years.