Loddon Homes Limited
Data Protection Policy

Contents

Page Number

1	Policy	1
2	Purpose	1
3	Scope	1
4	Principles	1
5	Review	1
6	Application	2
7	Policy Statement	2
8	Equality Impact Assessment	6
9	Glossary of Terms	7

1. Policy

This policy sets out how Loddon Homes Limited (LHL / the Company) will comply and work with the data protection legislation to store and process data fairly and lawfully.

2. Purpose

The purpose of this policy is to ensure that the Company complies with the eight principles of the Data Protection Act 1998 as outlined in 7.3.

The Data Protection Act regulates the processing of information relating to individuals. This includes obtaining, storing, using and disclosing such information. The act covers all data whether on paper, in computer files or recorded on other material. It also includes Closed Circuit Television (CCTV) images.

3. Scope

This policy applies throughout the Company and must be adhered to by all employees, Board Members, contractors (whether working in the Company offices or its homes), consultants and any other person granted access to data held or processed by the Company.

4. Principles

The following principles will apply to this policy, it will:

- be open, fair and transparent
- promote consistency in the approach for all customers
- reflect the Company's employees, customers and Board members' views
- be realistic, achievable and deliver value for money.

5. Review

This policy will be reviewed along with procedures and employees training needs at least once every year to ensure that it continues to operate within best practice guidelines

The policy and associated procedures will be reviewed if necessary due to any changes legislation.

Wokingham Housing Limited (WHL) officers will be responsible for ensuring that policy reviews are undertaken, that appropriate consultation takes place and that revisions are reported to the Board for its approval

6. Application

The Board will approve this policy and delegate responsibility to the WHL officers for ensuring that this policy is communicated and implemented.

WHL officers will provide / arrange for training of employees to ensure that they fully understand the wider issues surrounding this policy and associated procedures.

7. Policy Statement

Summary
7.1 Responsibility
7.2 Glossary
7.3 Principles of the Data Protection Act
7.4 Subject Consent
7.5 Disclosure
7.6 Right to access of information
7.7 Data security
7.8 Data retention and disposal
7.9 Training
7.10 Equality and diversity

7.1 Responsibility

It is the responsibility of all employees, Board members, consultants, contractor and sub-contractors (see Scope at paragraph 3) to maintain confidentiality and ensure they deliver their service in accordance with this policy.

A breach of confidentiality can be a serious offence and may lead to disciplinary action or even criminal prosecution. All employees should inform their line manager or another senior manager of any suspected breach of confidentiality or loss of data.

It is the responsibility of WHL team directors to ensure that team members are following the Data Protection Procedures.

The Managing Director is responsible for ensuring overall compliance with this policy and the Data Protection Act.

7.2. Glossary

This document refers to a number of specific terms from the Data Protection Act. Please see the glossary at the end of this document for an explanation of these terms.

7.3 Principles of the Data Protection Act

The eight data protection principles state that data must be:

- Processed fairly and lawfully;
- Be obtained only for one or more specified and lawful purpose;
- Adequate, relevant and not excessive for the purposes defined;
- Accurate and where necessary, kept up to date;
- Not kept longer than is necessary;
- Processed in accordance with the data subject's rights;
- Kept secure with measures taken to protect against unauthorised or unlawful use, accidental loss, destruction or damage;
- Not transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection in the opinion of the Information Commissioner.

The Act makes a distinction between 'personal data' and 'sensitive personal data' and all data processors must be aware of the difference between the two and the conditions for processing each of them.

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

- That data;
- 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, any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade Union membership;

- Physical or mental health;
- Sexual life;
- Criminal proceedings or convictions.

7.4 Subject Consent

When collecting information from a data subject, the Company should always inform them why the information is required and the use to which it will be put.

The Company collects information on a 'need to know' basis. This means that only information that is necessary for service provision, decision making, effective management and planning should be collected and stored. Once a need to know basis has been established it is not generally necessary to obtain the informed consent of the data subject to process the information.

Informed consent will be obtained from all individuals where sensitive personal data is processed.

The Company may process sensitive personal data for the purposes of satisfying operational and legal obligations such as the management of a tenancy and Company policies such as health and safety and equality and diversity

7.5 Disclosure

Data held by The Company will only be passed to other organisations on a need to know basis and with an individual's consent unless there are exceptional circumstances. Exceptional circumstances include:

- Where there is clear evidence of fraud;
- To comply with the law;
- In connection with legal proceedings;
- Where it would be essential for the Company to carry out its duties, for example, where the health and safety of an individual would be at risk by not disclosing the information or where there is a legal requirement to do so;
- Anonymously for statistical or research purposes.

Steps will be taken to confirm the identity of any person requesting information about themselves and will also be taken to confirm the identity of any other person representing another organisation and requesting information about another individual.

Where a request for data is made, the Company will check why the data is required and to whom that party intends to disclose it. This will ensure that such disclosure is in line with the Company's notification to the Information Commissioner

7.6 Rights to access of information

All past and prospective employees, employment applicants, Board Members, tenants, and suppliers (including contractors and consultants) and anyone else with whom the Company communicates are entitled to:

- Be informed that processing of their data is being undertaken;
- Ask what information the company holds about them, either electronically or in a manual system, and why it is held;
- Ask how to gain access to their personal information;
- Prevent processing of their personal information in certain circumstances;
- Correct, block or erase information which is regarded as wrong information;
- Be told how their information is kept secure;
- Be informed as to what the Company is doing to comply with its obligations under the Data Protection Act.

The Company will consider a request for information providing the request is in writing, and accompanied by proof of identification (if relevant). The Company reserves the right to charge a maximum fee of £10 for each subject access request as permitted by the Data Protection Act. The Company must provide the information within 40 calendar days of receiving the request and payment.

7.7 Data Security

The Company will ensure that all data, whether manual or electronic, is kept secure by taking precautions against physical loss or damage and restricting both access and disclosure.

Anyone processing data on behalf of the Company (including Employees) is responsible for ensuring that:

- Any personal data which they hold is kept securely;
- Personal information is not disclosed either verbally, in writing or otherwise to any authorised or unauthorised third party.

7.8 Data retention and disposal

The Company will keep different types of information for longer than others. All employees are responsible for ensuring that information is not kept for longer than necessary in accordance with the Company Document Retention Policy.

Where personal and confidential information is no longer required, it will be destroyed in a secure manner.

7.9 Training

This policy and the associated procedures and guidelines will be available for all employees. It will also be issued when there are any amendments to the policy.

Further in-depth training can be provided for employees who have extra responsibilities for data protection or who need extra clarification on what the Data Protection Act means for them.

Training on this policy and accompanying procedure will be covered as part of the induction process for all new starters.

7.10 Equality and Diversity

The Company is committed to ensuring the elimination of discrimination in all areas of its work. All customers should expect, and receive, equal standards of service delivery regardless of age, disability, gender, race, religion or belief, sexual orientation or transgender status. This equality of standards also applies to the handling of personal and confidential information.

8. Equality Impact Assessment

8.1 Who has been consulted in developing the Policy?

Date	Consultation methodology	Challenge/impact/result

Next review date	
June 2017	
Author Karen Howick	**Related Documents**
Karen.howick@wokingham.gov.uk 01189746952	

9. Glossary

Data Information being processed automatically or recorded manually as part of a relevant filing system, or recorded with the intention of doing either of the above.

Data Controller/Processor The person / organisation who determines the purpose and manner in which personal data is held and processed (e.g. the Company)

Data Subject The individual who is the subject of personal data (e.g. the tenant)

Personal Data Data (including facts and opinions) which relates to a living individual who is identifiable from that data. (Consent from data subject is needed)

Sensitive Personal Data Data containing information relating to an individual's:

- Racial or ethnic origins;
- Political Opinions;
- Religious or similar beliefs;
- Membership of a trade union;
- Physical or mental health condition;
- Sexual Life;
- (Alleged) commission of any offence.

(Explicit consent is needed)

Processing Obtaining, recording, disclosing, holding, consultation, using information or data, carrying out any operation on the information or data including erasure, destruction and retrieval

Consent Permission given

Informed Consent Unambiguous permission given via a positive action by the individual.