

South Western Housing Society Ltd
Data Protection Policy & Compliance

1. Statement of Intent

The Society aims to comply with the legal requirements of the Data Protection Act 1984, the Data Protection Act 1998 and subsequent legislation. The Society recognizes that personal information is confidential and that unauthorized disclosure is a breach of contract and an offence under the Data Protection Acts.

2. Background

The Data Protection Act 1998 came into force on 1 March 2000. The Act sets rules for processing personal information and applies to some paper records as well as those held on computers. Whenever personal data is collected and used, people's lives can be adversely affected if something goes wrong and, if data is not kept securely, people's privacy can be affected. It is vital that those who collect and use personal data maintain the confidence of those who are asked to provide it and this is assured by complying with the requirements of the Data Protection Act.

This policy explains how the Society will fulfill its duties and obligations under the Act with regard to its tenants and leaseholders, past and present.

3. Implementation.

The Society will implement the following actions in pursuance of its data protection policy.

3.1 Registration

The Society will ensure that it registers appropriately with the Information Commissioner. All new systems, where appropriate, will be registered immediately they become operational.

3.2 Staff

A guide to the Data Protection Act will be issued to all employees and further training provided where necessary. The Society will expect compliance with the Acts.

All staff involved in the processing and handling of data will receive training on the Acts. Disciplinary action will be taken against staff contravening the Acts.

3.3 Data Systems

All systems using personal data will be identified and their uses registered as required by the Data Protection Register. All systems will take into account the eight data protection principals.

4. The Data Protection Act – Eight Principles

The Data Protection Act applies to 'personal data' that is, data about identifiable living individuals, and covers both facts and opinions about them.

Those who decide how and why personal data are processed are known as Data Co-ordinators and their role is to ensure compliance with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act. The Society has nominated the Corporate Services Manager to act as Data Co-ordinator.

The eight enforceable principles of good practice say that data must be:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in line with the data subject's rights;
- secure;
- not transferred to countries without adequate protection

5. Definitions of Data from the Act

5.1 Personal Data – Section 1(1) - "data which relate to a living individual who can be identified:-

- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller;
- and includes any 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".

5.2 Sensitive Personal Data - "personal data consisting of information as to:-

- the racial or ethnic origin of the data subject;
- his/her political opinions;
- his/her religious beliefs or other beliefs of a similar nature;
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- his/her physical or mental health or condition;
- his/her sexual life;
- the commission or alleged commission by him/her of any offence; or
- any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

5.3 Data subject means a person about whom data is kept.

6. Relevant Filing Systems

The Data Protection Act covers information which is recorded as part of a 'relevant filing system', that is, a set of information in which the records are structured, either by reference to individuals or by reference to criteria relating to individuals, so that 'specific information relating to a particular individual is readily accessible'. The definition means a significant amount of manual data, as well as computerised records, fall under the scope of the Data Protection Act.

7. Security

7.1 Data Co-ordinators must take security measures to safeguard personal data. The 1998 Act requires that Data Co-ordinators must take appropriate technical or organisational measures to prevent the unauthorised or unlawful processing, or disclosure, of data.

7.2 Computer files will only be accessible to those with the right to process the data concerned and systems will be password protected for added security.

7.3 In addition, the Society encourages all staff to file relevant information to prevent unauthorised access to personal or sensitive personal data.

7.4 Sensitive personal data held in manual files will always be clearly marked "Confidential".

8. Transfer of Personal Data Overseas

The eighth principle restricts the transfer of personal data outside the European Economic Area (which consists of Norway, Iceland and

Liechtenstein as well as the European Union Member States). Personal data may only be transferred to third countries if those countries ensure an "adequate level of protection for the rights and freedoms of data subjects" or if the data subject has explicitly authorised the disclosure.

7. Notification

The Data Co-ordinator will notify the Commissioner, in broad terms, of the purposes of the processing, the personal data processed, the recipients of the personal data processed and the places overseas to which the data are transferred. This information is made publicly available in a register and will be renewed annually.

8. The Rights of Individuals

8.1 The Right of Subject Access

The Data Protection Act allows individuals to find out what information is held about themselves on computer and some paper records. This is known as the right of subject access. The Housing Manager is responsible for such files and for ensuring their safekeeping.

8.2 A tenant's or leaseholder's file will only be made available to:

- The individual concerned;
- Staff within the Society who require it in order to provide tenant/leaseholder services;
- Investigating Officers & representatives as appropriate when formal proceedings are entered into;
- Third parties with the explicit written consent of the tenant/leaseholder;
- Board Members dealing with complaints or appeals.

8.3 Accessing, disclosing or otherwise using records without authority will be treated as a serious disciplinary offence. Additionally, such conduct may constitute a criminal offence.

8.4 Should a tenant or leaseholder wish to view his/her file, they should make a written request to the Corporate Services Manager, providing a description of the information they wish to access and any other relevant details. The request will be acknowledged on the day of receipt and the information will be provided, or access to it made available, within 28 days. The Corporate Services Manager will retain a log of all such requests. The Society reserves the right to make a

charge for this service. This right is explained to all tenants in the tenant handbook,

- 8.5 Tenants and leaseholders will be asked to provide proof of identity, for example, passport, driving licence or birth certificate on the day of viewing. The inspection must take place within a Society office and in the presence of the Corporate Services Manager. All papers must be kept in the same order in which they appear in the file and no data may be removed or copied without permission.
- 8.6 The Society reserves the right to remove those items from personal files to which tenants and leaseholders do not have the right of access, e.g.
- Where information was supplied for the purpose of establishing a contract;
 - Where information that is held may be used for the purposes of preventing or detecting crime;
 - Where the information that is held has been supplied by a third party who has not given their consent for the tenant or leaseholder to view that information;
 - Where references have been supplied by a third party in confidence.
- 8.7 Joint tenants do not have a right of access to information held about each other as individuals.

9. The Right of Rectification, Blocking, Erasure and Destruction

- 9.1 The Data Protection Act allows individuals to apply to the Court to order a Data Co-ordinator to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.
- 9.2 Should any tenant or leaseholder disagree with an item being included in their file they should notify the Corporate Services Manager, in writing, so that a decision regarding the item can be made. Should the request to alter/amend a file be refused the tenant or leaseholder will be notified in writing of the reasons for such a decision. If they do not agree with the decision the matter can be pursued under the Complaints Policy.
- 9.3 In addition, tenants/leaseholders are required to notify the Society of any changes to the information that they have provided as and when the change occurs.

10. The Right to Prevent Processing

10.1 A data subject can ask the Data Co-ordinator to stop or request that they do not begin processing data relating to him or her where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to themselves or anyone else. However, this right is not available in all cases and Data Co-ordinators do not always have to comply with the request.

10.2 'Processing' is broadly defined and takes place when any operation or set of operations is carried out on personal data. The Act requires that personal data be processed "fairly and lawfully". Personal data will not be considered to be processed fairly unless certain conditions are met.

10.3 Processing may only be carried out where one of the following conditions has been met:

- the data subject has given his or her consent to the processing;
- the processing is necessary for the performance of a contract with the individual;
- the processing is required under a legal obligation;
- the processing is necessary to protect the vital interests of the individual;
- the processing is necessary to carry out public functions;
- the processing is necessary in order to pursue the legitimate interests of the Company or third parties (unless it could prejudice the interests of the individual).

10.4 Sensitive personal data can only be processed under strict conditions, which include:

- having the explicit consent of the data subject;
- being required by law to process the data;
- needing to process the information in order to protect the vital interests of the data subject or another;
- dealing with the administration of justice or legal proceedings.

11. The Right to Prevent Processing for Direct Marketing

A data subject can require a Data Co-ordinator to stop or not to begin processing data relating to him or her for direct marketing purposes. This is an absolute right.

12. The Right to Compensation

12.1 A data subject can claim compensation from a Data Co-ordinator for "damage" or "damage and distress" caused by any breach of the Data Protection Act. Compensation for distress alone can only be claimed in limited circumstances.

12.2 Any requests for compensation must be made in writing to the Corporate Services Manager detailing the situation that has given rise to the "damage" or "damage and distress" and the consequences suffered. The Corporate Services Manager will acknowledge such a request on the day of receipt and a decision will be made and communicated to the applicant within 28 days of the request.

13 . Rights in Relation to Automated Decision-Taking

13.1 A data subject can ask a Data Co-ordinator to ensure that no decision which significantly affects them is based solely on processing his or her personal data by automatic means.

14. Consent to Process

14.1 In order to comply with the legislation the Society requires a record of its tenants' and leaseholders' consent to hold, use and disclose personal and sensitive personal data about them for the purposes of managing and administering their tenancy and for the purposes of the Society's business.

14.2 The Society will not reveal information about tenants or leaseholders to anyone or use information about them for other purposes unless the law allows it to. A copy of the Company's Data Protection registration, which outlines the purposes for which data will be used and disclosures made, is available upon request to the Corporate Services Manager.

14.3 Tenants and leaseholders agree, by virtue of their tenancy agreement or lease, to the Society processing such information as may be necessary for the proper administration of the relationship,

both during and after the tenancy, provided that proper regard is paid to such data protection principles as may be in force.

15. Using the Data

The information that is held by the Society will only be used for legitimate purposes including:

- Managing any legal relationship (eg landlord and tenant) between the Society and the data subject and enforcing the Society's rights under that relationship;
- complying with obligations to tenants and leaseholders;
- complying with statutory obligations under general law, for example in relation to taxation, social security, or law enforcement;
- administration and payment of any amounts payable;
- providing information about tenants and/or leaseholders to those who require it in connection with services that they provide to the Society, or the Society to them, or who do (or may) own (or invest) in the Society;
- the prosecution or defence of any legal proceedings;
- monitoring as required by internal and external agencies, particularly for statistical and analytical purposes;
- audit purposes;
- compliance with equal opportunities policy;
- compliance with the Disability Discrimination Act;
- carrying out checks through Criminal Records Bureau, List 99 or other appropriate mechanisms.

When a tenancy ceases, all personal and sensitive personal data relating to that individual will be archived.

15. Disclosure of Data

15.1 Personal data, and in some instances sensitive personal data, will be disclosed to agents and third parties who provide functions on behalf of the Society and to those with a legitimate reason for receiving it to enable the above purposes to be carried out, e.g. external advisors, insurers, bankers, investors, Inland Revenue, healthcare providers, etc

15.2 Where third parties request either personal or sensitive personal tenant and/or leaseholder data, written signed authorisation must be obtained before information is shared with the third party. The authorisation will contain their name and address together with a description of what is required and any other details. The Society reserves the right to make a charge for the provision of information, which will be provided within 28 days of receipt of the written

request. A log of all such requests will be maintained by the Corporate Services Manager and/or Housing Manager as appropriate.

- 15.3 All employees and Board Directors should be aware that it is a criminal offence to access or disclose personal data held by the Society without authority.
- 15.4 Where those requiring the information maintain the employer is under a legal duty to respond, the Corporate Services Manager and/or Housing Manager will check to ascertain this is valid. Crime and taxation exemptions may be relied upon at times. In exceptional circumstances advice will be sought from legal experts and/or the Information Commissioner.
- 15.5 Third parties who wish to get in touch with data subjects including tenants, leaseholders and staff will be advised that the Society may be prepared to pass on correspondence, but will not disclose the data subject's address without their written consent.

16. Responsibility

It is the responsibility of the data controller to ensure compliance with this policy and to arrange training where appropriate.

It is the responsibility of the Corporate Services Manager in liaison with the Chief Executive to undertake a periodic review of files to ensure that no information is being kept longer than necessary.