



POLICY DOCUMENT

Data Protection Policy

POLICY TITLE:	Data Protection Policy
LEAD OFFICER:	Linda Milan
DATE APPROVED:	28 July 2010
APPROVED BY:	Corporate Services Committee and SLHD Board
DATE FOR NEXT REVIEW:	October 2011
ADDITIONAL GUIDANCE:	Freedom of Information Policy Acceptable Use Policy (Information and ICT equipment)
TEAMS AFFECTED:	All SLHD staff and Board members
THIS POLICY REPLACES WITH IMMEDIATE EFFECT:	Data Protection Policy v3 approved December 2009 Confidentiality Policy approved in June 2006

DOCUMENT CONTROL

For guidance on completing this section please refer to the document version control guidance notes

Revision History

Date of this revision:	28 July 2010
Date of next review:	October 2011
Responsible Officer:	IT Strategy & Systems Advisor

Version Number	Version Date	Author/Group commenting	Summary of Changes
V1	2005		
V2	2006		
V2.1	Sep 09	L Milan	Revised draft
V3	Dec 09	Board	Approved by Board
V4.0	July 10		

Page	Version	Date	Author
Page 2 of 11	4.0	16/06/10	S Taylor
File Path			



POLICY DOCUMENT

Data Protection Policy

1. Introduction

- 1.1 St Leger Homes of Doncaster (SLHD) needs to collect personal data about their customers and staff in order to provide services appropriately and efficiently.
- 1.2 SLHD are committed to protecting all of the data it holds on individuals and fulfilling all of the duties placed upon it by the Data Protection Act 1998 (DPA).
- 1.3 The DPA makes it mandatory for SLHD to take appropriate measures to ensure personal data is processed fairly and lawfully and held securely.
- 1.4 SLHD will not share the data so held with other organisations without the consent of the customer or member of staff unless we are required to do so by law.
- 1.5 SLHD purpose for holding personal data and a general description of the categories of people and organisations to which we may disclose it are listed in the DPA Register. The register will be reviewed on a regular basis.

2. Purpose

- 2.1 The purpose of this policy is to:
- Ensure that all Board members and staff are aware of the principles of the Data Protection Act 1998 and how this may influence their role
 - Define the criteria and controls that must be applied throughout the company to ensure compliance with the legislation and good practice.

Page	Version	Date	Author
Page 3 of 11	4.0	16/06/10	S Taylor
File Path			

3. Scope

3.1 This policy identifies the main principles of the Data Protection Act that must be adhered to when processing personal information by or on behalf of the company. This will include all paper based and IT based information.

4. Responsibilities

4.1 This policy applies to all members of staff, board members and all contractors working on behalf of St. Leger Homes. All employees have an individual responsibility to maintain the security of held data. Failure to do so may result in prosecution of the individual and/or the company, which may result in fines being imposed on the individual and/or the company.

5. Policy

5.1 Glossary of Terms

To aid a better understanding of the terms used within this policy the following definitions have been provided.

- Processing – Most activities involving the data (this includes the obtaining recording or holding of the data; or carrying out any operation on the data including organising, adapting or amending the data, its retrieval, consultation and use of the data, disclosing and erasure or destruction of the data).
- Personal Data – Data relating to a living person who can be identified from the data or other information held by the data controller.
- Data Controller – person who determines the purposes for which the held personal data can be used and shared.

5.2 Data Protection Act 1998 (DPA)

The principles of the act require that the person data held by the company must be:

- Fairly and lawfully processed (not processed unless specific conditions are met)
- Processed for the purpose(s) obtained and not further processed in any manner incompatible with that purpose(s)
- Adequate (not excessive) & relevant
- Accurate and kept up to date
- Not kept longer than is necessary
- Processed in accordance the rights of data subjects
- Held in a secure manner
- Not transferred to countries not covered by adequate protection of the individuals rights

5.3 Compliance with the DPA

Page	Version	Date	Author
Page 4 of 11	4.0	16/06/10	S Taylor
File Path			

To comply with the principles of the DPA SLHD will:

- Collect and use data fairly and lawfully
- Meet the legal obligations to specify the purpose for which information is used
- Collect and process appropriate information only to the extent that is needed to fulfil operational needs or to comply with any legal requirements
- Ensure the quality of information used to:
 - Hold the data only for an appropriate length of time (as defined in the SLHD Policy and guidelines)
 - Ensure that data subjects are able to fully exercise their rights under the DPA. This will include:
 - The right to be informed that the processing is being undertaken
 - The right of access to their personal information
 - The right to prevent processing in certain circumstances
 - The right to correct, rectify, block or erase incorrect information
- Take appropriate security measures to safeguard personal information. This will include:
 - Access to computer records containing personal information will be restricted to those persons who need access in order to carry out their duties.
 - Personal information contained on paper files will be stored in locked cabinets and access restricted to those with a legitimate business need to access the data.
 - Instruct staff that material is not taken off site without express prior approval or stored on personal machines normally kept outside the workplace
- Ensure personal information is not transferred abroad without suitable safeguards

5.4 Data Protection Procedures

5.4.1 Information regarding their personal and the company's responsibilities under the Data Protection Act will be given to all employees at the time of their employment and will be refreshed from time to time.

5.4.2 Employees whose duties may include the receipt of requests for personal information will be provided with more in depth training during their employment. All staff will receive reminders of the importance of compliance with the act during team meeting and via the staff brief.

5.4.3 Information will not be shared with any person or organisation other than

Page	Version	Date	Author
Page 5 of 11	4.0	16/06/10	S Taylor
File Path			

where appropriate authorisation has been given or the law requires us to do so. Failure to comply with this requirement may lead to disciplinary actions.

5.4.4 **Storage of Information**

SLHD stores the majority of personal information electronically. The information is safeguarded by restricting the number of employees who are able to log on to each system to those who require the information in order to carry out their duties.

5.4.5 Each individual using any of the programmes sets their own unique password and this allows management the ability to investigate who has made entries or amended any of the information it contains.

5.4.6 All staff who have access to electronic records must comply with the Acceptable Use Policy (Information and ICT equipment). This policy includes comprehensive details about the use of strong and secure passwords, on Information security and also on Equipment security.

5.4.7 The Acceptable Use Policy details a series of measures to be taken in respect of the storage and security of both electronic and paper-based information. This includes the following specific guidelines for the correct use of all information, and employees shall not:

- transmit, transfer or disclose SLHD's confidential information to unauthorised people
- transmit or transfer confidential data on ANY media (e.g. paper, memory stick/pen drive, CD, DVD) unless absolutely necessary and only then, where appropriate, they have been properly virus checked and authorised. If there is a business case for transportability on non-paper media and the data is sensitive then it must be encrypted (it is important to note that from August 2010 all USB ports will be blocked to unauthorised USB devices).
- install software applications in any circumstances without permission via the SLH IT team.
- load electronic files onto SLHD equipment from media such as CDs, DVDs, memory sticks/pen drive, e-mail attachments, the Internet or any other source without prior authorisation
- intentionally interfere with the normal operation of the network i.e. uploading computer viruses
- examine, change, or use another person's files without prior authorisation
- use another person's access code to log onto the network
- store the organisation's personal or business information on 'C' drives on their computer unless a latest copy of the information is also stored on a server (please note documents on a 'C' drive will not be backed up as a matter of course).
- leave personal or business sensitive information on desks at the end of each day or when the office is not occupied. This type of information must be locked away in either pedestals, filing cabinets or dedicated lockable storage, which have been provided to

Page	Version	Date	Author
Page 6 of 11	4.0	16/06/10	S Taylor
File Path			

all staff, as appropriate

Storage of paper information

All staff must ensure that this information is protected by:

- Ensuring the information is stored in locked cabinets during out of hours periods
- By ensuring that where it is necessary to remove the documents from storage they should be treated with respect at all times and must not be left on desks, photocopiers etc in a manner which places the information in danger of misuse or viewing by unauthorised persons.
- Storing newly acquired information should be stored in appropriate files or cabinets as soon as possible.
- Consider converting paper information to electronically stored information as soon as possible.

Document retention

SLHD has a Document Retention Policy which is based on good practise and guidance from the Records Management Society of Great Britain. During 2010/2011 facilities are being introduced with the electronic document management system (Information @ Work) that will lead to the automatic *culling* of stored information based on the document type and date, in line with the Document Retention Policy. The company also holds records from the 1930's to 1994 on behalf of the Council on microfiche and there is a planned programme to convert this information into the Information @ Work system starting in Summer 2010. At the end of this programme it is intended that the microfiche records will be destroyed.

This impacts on the duty to provide requested information as in the information is available it should be produced but it is accepted that companies cannot produce information which has been disposed of appropriately and in accordance with an agree Document Retention Policy.

5.4.8 Requests for information

5.4.8.1 **Individual Customers** – There are many circumstances that may prompt a customer to seek confirmation of their personal position e.g. their banding within Choice Based Lettings, current rent position, history of a repair request etc.

5.4.8.2 Although reasonable care should be taken to ensure that any information is passed to the correct person the degree of confirmation may vary with the sensitivity of the data being requested. While it may be appropriate to request a verbal confirmation of the customers identity to answer a customer's request for confirmation of their Band within Choice Based Letting System a higher level of confirmation of identity is required to discuss a customers rent arrears. Employees should seek further clarification from their line Managers regarding appropriate identification working practices within their work areas.

Page	Version	Date	Author
Page 7 of 11	4.0	16/06/10	S Taylor
File Path			

- 5.4.8.3 Caution should be exercised at all times and if doubts remain regarding the right of the person requesting the information this should be referred to the team Manager. If further guidance is required this can be obtained from the Company Secretary.
- 5.4.8.4 Customers also have the right to request to view information held on their personal records. Customers making this request should be asked to put this in writing clearly explaining or listing the information they require (requests by E Mail are acceptable). A standard form has been produced for those customers who would find this more convenient. Customers will be given any assistance they require to request documentation. All requests will be passed to the Manager of the appropriate section.
- 5.4.8.5 The identity of the person requesting the information should be checked (if necessary the customers signature can be checked with previous information held on the EDM system (any difficulty please contact Support Services on 01302 862730).
- 5.4.8.6 Care must be taken that the information given does not infringe on the rights of other data subjects, information provided by or referring to a third party should not normally be disclosed.
- 5.4.8.7 Access to information requests relating to the Data Protection Act must be met within 40 days.
- 5.4.8.8 SLHD makes no charge for the provision of this information (although it is accepted that this is permissible under the legislation) preferring to consider this a customer service this mirrors the current DMBC no charge policy. In cases of exceptional volume this may give grounds for refusing this request.
- 5.4.8.9 **DMBC Councillors**
- 5.4.8.10 Any officer receiving an enquiry from a Councillor relating to an individual tenant or customer must record full details onto the CC on line database. This will allow us to keep accurate statistical information and also to identify recurring themes and decide any resultant changes in procedures.
- 5.4.8.11 Councillors contact St Leger Homes to make enquiries on behalf of their constituents. Although this would normally involve the customers completing an agreement for the information to be given the Information Commissioner has stated that we are allowed to pass information provided that the following criteria are met:
- The customer has requested the Councillor assistance
 - The customer lives within the Ward Boundaries of the Elected Member
 - The information is not required for political purposes
- 5.4.8.12 If in doubt or the information is of a particularly sensitive nature the employee may contact the data subject to confirm their agreement to release the information to the Councillor. A note of this should be included

Page	Version	Date	Author
Page 8 of 11	4.0	16/06/10	S Taylor
File Path			

onto the logged request on the CC Online IT system.

5.4.8.13 The response to a Councillors enquiry should not give any personal information other than that which the customer has given permission to disclose.

5.4.8.14 **Board Members** – Board Members have no formal right to receive information on individual customers unless a specific confidential report is presented to the Board for approval.

5.4.8.15 **Contractors** – All SLHD framework agreements contain a confidentiality clause preventing the disclosure of SLHD records without written agreement. The contract will include the provision that the information remains the property of St Leger Homes at all times and should be returned or destroyed by agreement at the end of the contract. Contractors will be bound by this Policy.

All other contractors are to be sent details of the terms and conditions relating to SLHD contracts including the requirement to keep any data protected information secure, to use it only for the agreed purpose, and to destroy the information as soon as it is no longer required.

All contractors will be informed that failure to comply with the terms and conditions may result in the contract being terminated and/or legal proceedings.

5.4.8.16 **Requests from employees** – Employees also have a right to ask to see any information recorded on their personal records. All records are held securely within the HR team and any employee wishing to see their personal records should contact the Assistant Director of Corporate Services. Employee information is stored in both paper files and also electronic records within the CHRIS IT system.

5.4.8.17 **Applications for employment** - Applications from successful candidates are transferred to the new employees personal records (please see above). All details of unsuccessful applications will be held for a maximum of 6 months. The information provided on an anonymous basis i.e. gender race etc will be retained in spreadsheet format for statistical purposes

5.4.8.18 **Other Agencies** – SLHD has a duty to share information with some other agencies e.g. the police where this can be shown to meet legislative requirements, i.e. for the detection and prevention of crime and in circumstances considered to be in the interests of the community.

5.4.8.19 Information will not normally be provided to an organisation with which we do not have a data sharing agreement (formal agreement between organisations) without the customers consent unless covered by the provisions of the Act.

5.4.8.20 Data Sharing Agreements are to be agreed by either a Director or an Assistant Director. The Company Secretary will keep a record of all such agreements.

Page	Version	Date	Author
Page 9 of 11	4.0	16/06/10	S Taylor
File Path			

5.4.9 **Breaches of Policy**

All employees have an individual responsibility to maintain the security of held data. Failure to do so may result in prosecution of the individual and/or the company, which may result in fines being imposed on the individual and/or the company.

Any proven breach of this policy will be reported to the Board.

5.4.10 **Further guidance**

Further guidance is obtainable from the Company Secretary on 01302 862703 and can be found on the Information Commissioners Website at www.informationcommissioner.gov.uk.

5.4.11 **Request for other information**

To request information of a more general nature, not already published, please see the SLHD separate Freedom of Information Policy.

6. Monitoring and Review

6.1 All requests for information under the DPA are recorded on CC online. Adherence to this policy will be monitored by means of "Mystery Shopping" and through periodic compliance checks.

All employees will be asked to comment on their Data Protection awareness in appraisals undertaken from 2010.

6.2 The policy and procedure on Data Protection will be reviewed on a scheduled agree basis.

7 Performance Standards

7.1 Requests for information under the DPA must be dealt with within 40 days. If it is not possible to provide the requested information within this time scale further advice should be sought from the Company Secretary.

7.2 Failure to comply with this Data Protection Policy or legislation will be reported to SLHD Board

8 Training

8.1 The Company secretary is responsible for ensuring that all new staff receives basis information into their responsibilities regarding Data Protection during their induction to the company.

8.2 Team Leaders and Mangers are responsible for ensuring that training appropriate to an individuals role is provided and refreshed in conjunction with the training and development team

Page	Version	Date	Author
Page 10 of 11	4.0	16/06/10	S Taylor
File Path			

8.3 Regular reminders regarding the individual and company's responsibilities will be included in the staff magazine.

8.4 Board members will receive training that is appropriate to their role

9. Partnership issues

9.1 For consistency and as outlined in the Memorandum of Articles of Association, SLHD Data Protection Policy is closely aligned to that of DMBC.

Page	Version	Date	Author
Page 11 of 11	4.0	16/06/10	S Taylor
File Path			