Data Protection Policy

Definitions

Data – Any information automatically processed or going to be automatically processed. This includes information contained within structured and unstructured manual files.

Personal Data – Information relating to a living identifiable individual.

Sensitive Personal Data – Information relating to an individual's race / ethnic origin, their political opinions, religion, trade union membership, health, sexual life, criminal or alleged offences.

Data Controller – Person (i.e. natural person or legal body such as a business or public authority) that decides manner in which, and purpose for which, personal data are processed; this is the co-operative.

Data Subject – An individual who is the subject of the personal data/information.

Data Processor – A person who processes on behalf of the data controller under instruction.

Processing – Any activity / operation performed on personal data – whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data. This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. It is difficult to envisage any activity, which does not amount to processing.

Information Commissioner – an independent Officer appointed by Her Majesty the Queen and who reports directly to Parliament.

1 Purpose of Data Protection Policy

Scope

It is the co-operative's obligation to ensure compliance with the Data Protection Act 1998. The Information Commissioner, who oversees compliance and promotes good practice, requires all data controllers who process personal data to be responsible for their processing activities and comply with the eight data protection principles of 'good information handling'.

These are:

1. Personal data shall be processed fairly & lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes
3. Personal data shall be adequate, relevant and not excessive
4. Personal data shall be accurate and, where necessary kept up to date
5. Personal data shall not be kept for longer than is necessary
6. Personal data shall be processed in accordance with the rights of data subjects
7. Security principle – Protection against unauthorised /unlawful processing
8. Transfers outside of the European Economic Area (EEA) – Requires adequate levels of protection

Data protection law and policy aims to ensure that individual's rights and freedoms are protected. Using personal data to abuse, discriminate or deny access to services is unlawful. The co-operative is committed to ensuring that personal data that it holds is used fairly and lawfully and in a non-discriminatory manner.

This policy applies to all personal data held by Southsea Self Help Housing Co-operative. It encompasses manual / paper records and personal data electronically processed including information gathered on CCTV systems, of whatever type and at whatever location.

Companies and organisations will hold information of a personal nature about people. If this information is collected or entered wrongly, is out of date or is mixed up with someone else's personal data, it could cause complications as a result.

2 Overview of the Data Protection Act 1998

The Data Protection Act 1998 gives individuals the right to see information about them held by companies and organisations. In certain circumstances they may have the information corrected or erased, or they may even be able to prevent the processing of their personal data. If a Data Controller causes an individual damage or distress as a result of non-compliance, they could claim compensation. The co-operative is classed as a Data Controller and could be prosecuted for any serious offences that may be committed.

The Data Protection Act 1998 is not optional. It is mandatory and there can be harsh penalties imposed for non-compliance with the Act. In a Crown Court fines can be unlimited and all organisations processing personal data can be affected.

The obligations outlined in this policy apply to all those who have access to personal data held by the co-operative, whether members, contractors or consultants. All individuals permitted to access personal data in line with their duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the position being undertaken.

3 Confidentiality and Security

Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles as defined in the Data Protection Act 1998.

- Manual files (paper records) – access must be restricted solely to relevant individuals and stored in secure locations (e.g. lockable cabinets), to prevent unauthorised access.
- Computer systems will be configured and computer files created with adequate security levels to preserve confidentiality. Those who use the co-operative's computer equipment will have access only to the data that is both necessary for the work they are doing and held for the purpose of carrying out that work.
- Personal data will be disclosed only to the data subject and other organisations and persons who are pre-defined as notified recipients within the co-operative's Notification Register Entry held with the Information Commissioners Office. At certain times it may be required that personal data is disclosed under one of the exemptions within the Data Protection Act 1998. If there is a requirement for this an audit trail

will need to be kept to provide accurate records of any disclosures of personal data.

- Preventing abuse and discrimination. The co-operative processes sensitive personal data (as defined in the Act) on members and will have regard to its various diversity policies to ensure that if instances of abuse or discrimination occur, appropriate action is taken

4 Obtaining, Recording, Using and Disclosing

4.1 Processing

Processing in relation to personal data means carrying out any of the processing activities "on the data". Any activity / operation performed on personal data – whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data.

This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. *(It is difficult to envisage any activity, which does not amount to processing)*

All processing of personal data will comply with the Data Protection Principles as defined in the Data Protection Act 1998. In the situation where a third party processes data, the third party will be required to act in a manner which ensures compliance with the Data Protection Act 1998 and have adequate safeguards in place to protect the personal data.

4.2 Recording and using the data

Data will only be processed for the purpose for which it was collected and should not be used for additional purposes without the consent of the data subject. The co-operative will endeavour to inform all individuals of why their personal data is being collected. In line with the first data protection principle all information will be collected fairly and lawfully and processed in line with the purpose for which it has been given. The co-operative may need to hold and process information in order to carry out any statutory obligations, where this process takes place all personal data will be processed fairly and lawfully.

4.3 Obtaining

It is a requirement that any data collection forms used in order to collect personal data will contain a "fair obtaining" statement. The statement will need to be clearly visible and placed appropriately so the data subject

(individual to whom the information relates) is fully aware of the intended uses of their personal data.

The information that would need to be supplied on a data collection form is as follows:

- The identity of the data controller or appointed representative
- The purpose or purposes for which the information is intended to be processed
- Any foreseen disclosures of the information to be obtained
- Any further information in order to make the processing fair.

It is also very important to remember that when collecting data via the telephone or face to face the above information should also be made clear to the data subject before any processing of their personal data takes place.

4.4 Disclosing

Personal data must not be disclosed, except to authorised users, other organisations and people who are pre-defined as a notified recipient or if required under one of the exemptions within the Data Protection Act 1998.

5 Data Subjects Rights

5.1 The Right of Subject Access (sections 7 to 9)

A written request received by a Data Controller from an individual wishing to access their rights under the provisions of the Data Protection Act 1998 is known as a Subject Access Request. Sections 7 to 9 of the Act gives an individual the rights to request access to any 'personal data' that they believe may be held about them. This can include requests from children under the age of 16 (or those acting on their behalf).

If it does hold the requested information, then it will provide a written copy of the information held about them and details of any disclosures which have been made. The information requested will be provided promptly and in any event within 40 calendar days of receipt of the subject access request. If the information cannot be disclosed within the time period specified, the data subject will be kept fully informed of the process and given access to any personal data that may already have been gathered.

If the Data Subject believes that co-operative has not responded correctly and is not happy with the co-operative's response to the concerns he / she is able to complain to the Information Commissioner.

5.2 Prevention of processing causing damage or distress (section 10)
If an individual believes that a Data Controller is processing personal data in a way that causes them substantial unwarranted damage or substantial unwarranted distress, they can send a notice (Data Subject Notice) to the Data Controller requesting, within a reasonable time, the Data Controller to stop the processing.

5.3 Right to compensation (section 13)
An individual who suffers damage, or damage and distress, as the result of any contravention of the requirements of the Act by a Data Controller, is entitled to compensation where the Data Controller is unable to prove that they had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

6 Use of Risk Markers

A Risk Marker is defined as: a measure of risk that the member represents to contractors, via any face to face or verbal interaction. This risk could be one or many of a wide range of factors such as risk of inflicting physical harm, or verbal abuse, or risk when visiting a location. The use of Risk Markers as a means of identifying and recording individuals who pose, or could possibly pose, a risk to the contractors who come into contact with them, is in practice, a flagged piece of text attached to an individual's file. These markers should be used very carefully and should contain the reasons for identifying individuals as presenting a risk. They are likely to record information relating to:

- The nature of the apparent risk posed by interaction with an individual
- Any threatening actions, incidents or behaviour they have or are alleged to have committed

The information relating to the creation and sharing of a 'flag' needs to be handled carefully taking into account security and confidentiality concerns. For the processing of this personal data to be fair, the Data Controller should normally inform individuals who have been identified as being a potential risk soon after a decision has been made to add a marker to their record setting out why their behaviour was unacceptable and how this has led to the marker.

The individual should be told:

- The nature of the threat or incident that led to the marker
- That their records will show the marker
- Who you may pass this information to
- When you will remove the marker or review the decision to add the marker.

There may be extreme cases where informing the individual would in itself create a substantial risk of a violent reaction from them, for example, because of the nature of the incident or the risk to another individual. In these cases it may not be sensible to inform the individual as described. If this is the case, the Data Controller must be able to show why they believe that by informing the individual of the marker there would be a substantial risk of further threatening behaviour.

7 Shielded Records

Shielded Records refer to the records of an individual who is at risk of physical or verbal harm in some way. Shielding refers to the withholding of the whereabouts and contact details of an individual and is only applied where there are strong reasons to do so, for example, where a practitioner has reason to believe in their professional opinion that not doing so is likely to, for example:

- Place a child at increased risk of significant harm
- Put a child's placement at risk (in the case of adoption)
- Place an adult at risk of serious harm
- Prejudice the prevention of a serious crime