

Data Protection and Confidentiality Policy. 8/12/2020

This policy supersedes the whole of the Confidentiality Policy dated 25 November 2013.

All co-op members and employees are entitled to access information concerning them held by Seymour Housing Co-operative (“the Co-op”) in accordance with the Data Protection Act 2018 and the Freedom of Information Act 2000. Others may request any information about them that the Co-op holds.

All employees, contractors, Management Committee members and others are responsible for the safeguarding of information to which they have access, including ensuring that it does not fall into the hands of any unauthorised person.

1. General

1.1 The Management Committee of the Co-op shall at its first meeting following each Annual General Meeting appoint a Data Protection Officer. In case of need the functions of the Data Protection Officer shall be exercised by the Secretary.

1.2 Definition of “confidential information”

The co-op holds two forms of confidential information. These are:

- Information held regarding the personal circumstances of individual tenants and applicants; and
- Information held on the employment files of the co-op’s staff members

Employees, contractors and volunteers need to be aware that some of this data may fall into the “special categories of personal data” defined in data protection legislation. The effect of this is that the Co-op is subject to more stringent conditions on holding and processing this than for other personal data. Rather than go into definitions, it is the policy of the Co-op to afford all personal data the same level of protection that the special categories of personal data require.

1.3 The Co-op may hold or process personal data for the purposes of safeguarding of economic well-being of individuals; safeguarding of children and of individuals at risk; offering support for individuals with a particular disability or medical condition; preventing fraud; preventing or detecting unlawful acts; promoting racial and ethnic diversity; promoting equality of opportunity or treatment; or for statutory purposes.

2. Access to confidential information

2.1 Information held on tenancy files shall remain at all times confidential and open only to staff and Management Committee members to view when they have a need to do so in order to fulfil their duties; see also paragraph 5 below.

2.2 Information held on employment files shall at all times remain confidential and open only to the staff member’s employer – that is to members of the Management Committee and the Line Manager – when they have a need to do so in order to fulfil their duties.

2.3 Other members of the co-op acting as members of sub-committees or panels may be given access to confidential information on occasions, and for limited periods, by the Management Committee, or in urgent cases by Chair’s action. In such cases, restrictions may be placed on access to confidential information.

- 2.4 Those authorised to have access to confidential information remain bound by the terms of this policy after their authorisation has ended.
- 2.5 Those authorised will under no circumstances communicate confidential information to any unauthorised person.
- 2.6 Anyone breaching the terms of this policy will automatically cease to be a member of the Management Committee and / or any sub-committee or panel for an agreed period of time dependent upon the severity of the breach.
- 2.7 Employees' and contractors' contracts with the Co-op shall specify their duties to prevent breach of confidentiality and comply with this policy.
- 2.8 Should there be a conflict regarding access to confidential information, the final decision rests with the Data Protection Officer.

3. Recording, storing, protecting and communicating confidential info

- 3.1 Confidential information will be recorded, stored and communicated in a secure manner that ensures it cannot be accessed by unauthorised people and is in accordance with current legislation.
- 3.2 Discussions involving confidential information must take place in the absence of unauthorised people. The Management Committee should aim to deal with all confidential business on a particular agenda consecutively, preferably at the beginning or the end of the Management Committee meeting.
- 3.3 All employees, contractors, members of the Management Committee, members of any sub-committee or panel or other volunteers will be issued with a copy of this policy and required to sign that they have read it, understand it and agree to abide by it.

4. Reporting breaches

Any person who becomes aware of any breach or fault that may have led to personal data being available to unauthorised persons must contact the Data Protection Officer within 24 hours of becoming aware of it.

5. Subject Access Requests and other data requests

Any request purporting to be a Subject Access Request and any other request or demand to provide any individual's personal information will be referred immediately to the Data Protection Officer and no other person will make any response to it. It is the responsibility of the Data Protection Officer to take all steps necessary to verify the identity of the requester and all other steps necessary to dealing securely with the request.

6. Retention of data

The Co-op shall retain personal data for no longer than is required for the purposes of its management and accounting or for the purposes listed in paragraph 1.3 above.