

Tenants First Housing Co-operative  
Data Protection and Access to Personal Information Policy

***Approval date: July 2009***

***Review Date: July 2012***

INDEX

1. Introduction.....	2
2. Data Protection Principles .....	2
3. Data Held.....	4
4. Sensitive Data .....	4
5. Information Commissioner- Notification .....	5
6. Compliance .....	5
7. Access to Personal Data .....	6
8. Confidentiality.....	7
9. Security .....	7
10. Training.....	7
11. Complaints.....	8
12. Equal Opportunities .....	8
13. Monitoring and Reporting .....	8
14. Review .....	8
15. Legal.....	8
16. References .....	9
17. Associated Policies/Documents.....	9
APPENDIX 1 .....	10
APPENDIX 1 .....	12
APPENDIX 1 .....	14
APPENDIX 1 .....	16

[Return to Main Policy Index](#)

## **1. Introduction**

Tenants First Housing Co-operative recognises that the Data Protection Act 1998 is an important piece of legislation to protect the rights of individuals in respect of any personal information that we keep about them, whether on computer or in manual systems.

The Co-operative is required by law to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective members, employees and others with whom it communicates. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data Protection Act 1998.

Guiding Standards 3.5 and 4.4 of the Scottish Housing Regulator Performance Standards state that “We are open about what we do and publish information about our activities. We provide information that people ask for, unless there are justifiable reasons for withholding it” The Co-operative regards the lawful and correct treatment of personal information by it as very important to effective operations, and to maintaining confidence between Tenants First and those it deals with. The Co-operative will ensure that it treats personal information lawfully and correctly, and take steps to safely destroy any information which is no longer relevant in law.

## **2. Data Protection Principles**

The Co-operative will adopt and operate procedures in accordance with the eight Data Protection Act principles. These principles require that personal information held by the Co-operative:

1. shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
2. shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4. shall be accurate and, where necessary, kept up to date;
5. shall not be kept for longer than is necessary for that purpose or those purposes;

6. shall be processed in accordance with the rights of data subjects under the Act;

and that:

7. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

8. shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Therefore, Tenant First Housing Co-operative will:

- fully observe conditions regarding the fair collection and use of information;
- meet the required legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken: the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct rectify, block or erase information which is regarded as wrong information.);
- take appropriate security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards.

The Co-operative and all staff who have access to any personal information must ensure that they follow the Data Protection Principles at all times. Training will be provided on these principles and the Co-operative's procedures for all relevant staff on a regular basis. New staff will have this incorporated into their induction process.

### 3. Data Held

The Co-operative will hold data record sheets for each data subject group (for example prospective members, members, former members, prospective employees, employees, former employees, committee members). These will ascertain:

- the nature of the information to be held
- the purposes that it can be used for
- the retention period for information
- how often the data should be checked- if relevant
- who the recipients of the data will be

These will be reviewed on a regular basis to ensure there is a sound business reason for this information to be retained.

Data subjects will be advised of the nature of the data the Co-operative is holding on them, its purpose and to whom the data may be disclosed.

Information can be held in a variety of formats eg:

- Databases
- Spreadsheets
- Manual records and files
- Computerised files and records
- E-mail. The Co-operative processes information which identifies individuals via e-mail correspondence. In order to minimise the risks associated with this, and in accordance with ICT Policy a disclaimer is contained within each staff members' e-mail signature which must be used with all external messages.

### 4. Sensitive Data

In order to obtain and process personal sensitive data, the Co-operative must obtain the individual's **explicit** consent. The DPA defines the following as "sensitive data"

- Racial or ethnic origin
- Political opinions
- Religious beliefs, or beliefs of a similar nature
- Membership of a Trade Union
- Physical or mental health or condition
- Sexual life
- The commission or alleged commission by them of any offence

- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

However, **explicit** consent is not required if:

- It is necessary in respect to legally imposed employment rights and obligations
- It is already publically available due to actions of the data subject
- It is necessary for legal proceedings, eg anti-social behaviour, for government or statutory functions
- It is for equal opportunities monitoring

## **5. Information Commissioner- Notification**

The Co-operative will review its registration with the Information Commissioner on at least an annual basis to ensure it accurately records:

- The purposes for which personal information is held
- Who the data subjects are we are holding personal information on
- The types of data class we are holding
- The sources of the personal information we are holding
- The recipients of the personal information we are holding

## **6. Compliance**

1. The Chief Executive has overall responsibility for data protection within the Co-operative.
2. The IT Supervisor will register the Co-operative as a Data Controller under the Data Protection Act with the Information Commissioner.
3. The IT Supervisor will ensure that our notification to the Information Commissioner and our entry in the Data Protection register is up to date.
4. Line managers will ensure that personal data processed by their section is included in the Co-operative's data protection register entry, is kept up to date and complies with the above principles. Any data not included in the current registration should not be processed until the notification is amended.
5. The Corporate Service Manager will implement the requirements of the Act by:

- co-ordinating staff training requirements on at least an annual basis
  - providing advice and support to all sections on all matters relating to compliance with the Act.
  - disseminating information relating to the Act.
  - responding to requests from individuals to access personal information we hold about them.
6. The Corporate Services Manager has specific responsibility for personal information held on employees. Staff will be informed about data protection issues, and their rights to access their own personal data. All personnel data will be kept in a locked filing cabinet, under control of the Corporate Services Manager. Personnel information held electronically will have restricted access on a "need to know" basis.
  7. All staff have a responsibility to fully comply with the requirements of the Data Protection Act and this policy. When involved in requesting information, staff will explain why the information is necessary, what it is to be used for, and who will have access to it.
  8. All staff should be aware that access to personal information includes information given in writing, by e-mail and over the phone.
  9. Serious breaches of the Data Protection policy and/or procedures will be regarded as Gross Misconduct and will render the employee liable for dismissal without notice.

## **7. Access to Personal Data**

Members, former members, applicants, employees and anyone else the Co-operative holds personal information on have the right of access to such information unless exemptions under the Data Protection Act apply.

We will respond to access requests as promptly as possible and certainly within the 40 day limit laid down in the Act.

The Co-operative will not normally charge for requests for information. However The Co-operative reserves the right to make a charge of £10 to cover administration costs where it is felt necessary to do so.

Please note that applicants for housing have the right to check information they have provided in connection with their housing application free of charge.

## **8. Confidentiality**

This policy complements the Co-operative's Openness and Confidentiality policy. Only information which can or must be legally disclosed under the Data Protection Act will be shared with a third party without the individuals consent. Employees and Committee members will be obliged to sign a confidentiality form and to agree to the security measures to ensure the security of personal information against unlawful processing, disclosure, accidental loss or destruction of, or damage to, personal data.

## **9. Security**

Security in relation to electronic information is covered in the ICT Policy.

Personal information held manually will be subject to measures to ensure against unlawful processing, disclosure, accidental loss, destruction or damage. **See Appendix 1.**

Staff should not leave personal information on their desk unattended. Particular care should also be taken in public areas and interview rooms.

All personal information being disposed of must be disposed as confidential waste.

Items sent to the secure company for archiving should be logged on the server before despatching for secure storage.

## **10. Training**

The Co-operative through its Internal Management Plan is committed to training and developing staff and committee members to their full potential in order to deliver a high quality of service in all areas of its business to tenant members and the public.

The employee induction programme includes an overview of this policy and refreshers will be held on at least an annual basis. Committee members and staff will receive updates on these issues and specific training on any specialised areas of equalities issues as required. Training needs are identified on an ongoing basis by various means including through the regular staff supervision sessions.

## **11. Complaints**

Should any applicant be dissatisfied with the way their data access application has been dealt with they may complain to the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Tel: 01625 545745 [www.ico.gov.uk](http://www.ico.gov.uk)

Where applicants are dissatisfied with the way their request for personal information has been dealt with and it falls outwith the scope of the Data Protection Act, they should make a complaint in accordance with the Co-operative's Complaints Policy.

## **12. Equal Opportunities**

The Co-operative will ensure that in implementing this Policy it will not unfairly discriminate against any individual, household or group on the grounds of gender, gender identity or marital status, on race grounds, or on the grounds of disability, age, sexual orientation, language or social origin, other personal attributes, including beliefs or opinions such as religious beliefs or political opinions.

## **13. Monitoring and Reporting**

Reports on the number of data subject access requests received and performance against target will be made to the Committee of Management.

The Committee of Management will be advised of any investigation by the Information Commissioner re alleged breaches of the legislation.

## **14. Review**

This Policy will be approved by the Finance and Corporate Services Sub Committee. It will be reviewed every three years unless amendment is prompted by a change in legislation or guidance which means that a change in Policy is required sooner.

## **15. Legal**

Data Protection Act 1998  
Human Rights Act 1998  
Freedom of Information Act 2000  
Crime and Disorder Act 1998  
Codes of Practice  
Housing Scotland Act 2001

## **16. References**

Communities Scotland Performance Standard: GS3.5 Openness and confidentiality

BSI: Data protection Guide

CCH: IT and e-Business management briefing

## **17. Associated Policies/Documents**

- ICT Policy
- Openness and Confidentiality Policy
- Monitoring Policy
- Data Subject Access Request Procedures
- Retention Guidelines
- Information Commissioner Registration
- Housing Benefit Service Level Agreement
- Archiving Procedure

## APPENDIX 1

### INFORMATION AUDIT – PERSONAL DATA

#### Section: Corporate Services/Compliance

**WHEN CARRYING OUT THE AUDIT THINK: -**

What is done with this information?

Why is it needed?

When was it stored or last updated?

Is it correct and up to date?

Is there duplication with other information held?

Is there justification for keeping the information?

Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed onto
Employees' personnel records	Locked cabinet, computer records.	Details of employment and next of kin, etc. for efficiency of organisation	While in employment (except spent disciplinary matters)	Details supplied for references, Inland Revenue, Police, Pension Scheme, DSS, Department of Employment, Auditors, SHR, Solicitors, Employee Counselling Service
Past Employees' personnel records	Locked cabinet, computer records	Reference for future employers, Pension companies Best practice	6 years after employment ceased	Other employers, Pensions, Police, Inland Revenue, DSS, Department of Employment, Auditors, SHR, Solicitors
Unsuccessful job applicants' application forms, interview records	Locked cabinet	In case of dispute/ Employment Tribunal or query on application	6 months	ACAS, Employment Tribunal, Lawyers acting for the Co-op
Parental Leave/Flexible working records	Computer records	IPD recommendation/ Inland Revenue requirement	18 years from child's birth	Inland Revenue
Accident or injury at work records/Accident books	Locked cabinet	In case of claims/ Legislative requirement	12 years	Insurers, legal advisers, H&S Executive
Register of Directors, Committee members names, address,	Computer records Locked cabinet	Regulatory requirement	Permanently	Auditors, SHR, solicitors
Declaration of interest forms	Computer records Locked cabinets	Regulatory requirement, In case of claims	6 years	Auditors, SHR, solicitors
Complaints to the Co-op and	Computer records	To monitor and record	Indefinitely	Ombudsman, Committee, Auditors, SHR,

the Ombudsman		complaints		other staff, members via newsletters (anonymous statistics only)
Medical records (H&S)	Computer records	Legislative requirement	40 years	Legal Advisers, H& S Executive, Insurers

## APPENDIX 1

### INFORMATION AUDIT – PERSONAL DATA

#### Sections: Property Management and Development

**WHEN CARRYING OUT THE AUDIT THINK: -**

What is done with this information?

Why is it needed?

When was it stored or last updated?

Is it correct and up to date?

Is there duplication with other information held?

Is there justification for keeping the information?

Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed onto
Telephone contacts, addresses & e-mail addresses of suppliers, contractors & other contacts	Telephone directories, address books (manual and computerised)	To be able to contact people	Indefinitely	Members, Committee members, Partner organisations
Repairs work orders & satisfaction surveys	Computer records	To keep record of individual repairs carried out in each property & for statistical reports	Indefinitely	SHR, Auditors
OT records (details of members' medical conditions)	Locked cabinet and computerised house file	To ensure appropriate adaptations carried out to property	Indefinitely	Internal use within company only
Medical records under the control of Asbestos <ul style="list-style-type: none"> <li>Medical records containing details of employees exposed to asbestos</li> <li>Medical examination certificates</li> </ul>	Locked cabinet and computerised personnel file	Statutory requirement	<ul style="list-style-type: none"> <li>40 years from date of last entry</li> <li>4 years from date of issue</li> </ul>	H&S Executive, Legal advisers, insurers, medical professionals
Medical records and details of biological tests under the control of lead	Locked cabinet and computerised personnel file	Statutory requirement	40 years	H&S Executive, Legal advisers, insurers, medical professionals
Medical records as specified by COSHH 1999	Locked cabinet and computerised personnel file	Statutory requirement	40 years	H&S Executive, Legal advisers, insurers, medical

				professionals
Medical records under Ionising Radiations Regulations 1999	Locked cabinet and computerised personnel file	Statutory requirements	Until the person reaches 75 years of age, but in any event for at least 50 years	H&S Executive, Legal advisers, insurers, medical professionals

## APPENDIX 1

### INFORMATION AUDIT – PERSONAL DATA

Department: **Housing Management**

**WHEN CARRYING OUT THE AUDIT THINK: -**

What is done with this information?

When was it stored or last updated?

Is there duplication with other information held?

Is there justification for keeping the information?

Why is it needed?

Is it correct and up to date?

Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed onto
Current housing applications	Held by Homehunt	To assess housing need to allocate houses fairly	Until allocation made or cancelled.	SHR & Committee (statistics only), Partner organisations.  Successful applications are transferred to Tenants First Cabinets and computer system.
Ethnic monitoring forms for housing list applications	Held by Homehunt	Reporting for APSR & Committee	Removed annually	Auditors, SHR and Committee (statistics only)
Cancelled housing applications	Held by Homehunt	To streamline housing list as historically applicants will respond some time after cut off period	6 months after date of cancellation	Committee (statistics only), Partner organisations
Member Files & Rent Account	Paper files & Computerised house files	To record rent payments, arrears and HB arrangements & to produce reports as well as record any other activity during tenancy	For duration of tenancy. Thereafter managed through Former Tenancy practices.	SHR, Auditors, Solicitors, Welfare Benefits Advisor, HB
Former Tenant Files	Computer records & paper files	To refer to in relation to tenancy reference requests from new landlords. Right to Buy applications.	<sup>1</sup> 12 months if no tenancy issues If there are tenancy issues such as abandonment, ASBO etc. then we hold for 5 years.	Other landlords
Anti-social complaint records	Computer records & paper	Statistical purposes or to	Indefinitely for statistics	SHR, Auditors, Solicitors

	records	monitor trends of specific complaints		
List of members	Computer records	Regulatory requirements, mail-outs,	Permanently	SHR & Committee (statistics),
Housing Benefit records	Computer records	In case of dispute	As <sup>1</sup> above	Local Authority, Benefits Adviser
Records re Sex Offenders	Held by Homehunt (Housing Manager's office)	SLA signed up to with local authority in relation to MAPPA, and data protection, requires us to keep any sensitive data secure and confidential	Until allocation made or cancelled	Local Authority Sex Offender Liaison Officer (SOLO), Criminal Justice, Police, other landlords (info provided on a restricted basis)
Housing Support Plans and associated documents.	Computer records & manual records held at schemes.	Care Commission requirements. Local authority contract requirements	Destroyed 6 months after tenancy ends.	Local Authorities, Health Professionals, next of kin

## APPENDIX 1

### INFORMATION AUDIT – PERSONAL DATA

Department: Finance

**WHEN CARRYING OUT THE AUDIT THINK: -**

What is done with this information?

Why is it needed?

When was it stored or last updated?

Is it correct and up to date?

Is there duplication with other information held?

Is there justification for keeping the information?

Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed onto
Invoices	Computer records, Lever arch files	Auditing purposes	6 years	Accountant, Auditors and SHR, Customs & Excise
Insurance claims	Computer records Locked cabinet	To monitor claims	7 years/2 years after settlement	Auditors, Insurers, Solicitors
Salary records, Tax, NI, Pensions, expenses, SSP, SMP etc	Computer records Locked cabinet	Inland Revenue and legal requirement	6 years	Inland Revenue, Auditors, Payroll agency, Pensions administering authority (ACC)
Rent/Service charge statements	Computer records	Regulatory requirement Best practice	2 years	Other landlords (payment history)
Schedule 7 issues under Housing (Scotland) Act 2001	Schedule 7 Register – computer	Statutory requirement	Indefinitely	SHR
Re-chargeable repairs	Computer records Locked cabinet	To record payments due and paid and action taken	7 years after debt cleared or written off	Auditors, other landlords (tenancy reference)
Annual Earnings summary	Computer records	Best practice	12 years	Auditors
Register of Share Certificates	Computer records	Legal Requirement	Indefinitely	SHR, Legal Advisers
Right to buy and Owners details	Disposal register	Statutory Obligation	Indefinitely	SHR, publicly available document

**Some of the older information above will be archived and held by a professional storage company in secure containers off company premises. Full archive records are held on com**