



## **DATA PROTECTION**

**Version 1**

**Category: Corporate**

**Latest Review Date: September 2014**

**Review Frequency: 3 years**

**Owner: Company Secretary**

**Contributors: Head of HR Services, Training & Development  
Manager, Head of IT, Housing Services Manager, Revenue Manager**

## **POLICY**

### **1. Policy Goal**

To protect the privacy of and promote the rights of individuals whose personal and confidential data is held by ECCT, whilst ensuring that ECCT has the necessary data to provide housing, care and well-being services to give older people an independent, safe and secure future in a network of inspirational communities and to manage its employees.

### **2. Business Objectives**

To ensure that data protection is considered as part of every business decision and is managed as integral part of ECCT's activities.

To protect and secure individual's formation whilst ensuring that information can be shared appropriately to meet legitimate business needs and comply with ECCT's Safeguarding Policy.

To meet the requirements of the Data Protection Act 1998 ("the Act") and regulatory guidelines in order to minimise the risk of enforcement action by regulatory bodies and diminution of reputation.

### **3. Organisational Statement**

As a responsible provider of housing, care, housing related support and associated services for people over 55 and as a responsible employer ECCT is committed to valuing the personal information entrusted to it and to respecting that trust by being open and transparent about how it uses, shares and protects personal information; ensuring that all its employees are trained to handle personal information appropriately.

### **4. Outcomes**

All ECCT trustees, staff, volunteers, residents, other service users and contractors are aware of this policy and adhere to all data protection procedures.

Mandatory training is provided to all relevant staff and volunteers on data protection, raising staff awareness of privacy issues.

Relevant and proportionate personal data is obtained, used, stored, disclosed and disposed of fairly and lawfully and only in accordance with the Act and safeguards are implemented and maintained to protect the accuracy and security of individual's personal data at all ECCT locations.

All individuals about whom personal data is held are aware of the identity of the data controller, the reasons why personal and sensitive personal information is required to be processed, how it will be processed, protected, securely disposed of and if, how, when and with whom data will be shared.

All subject access requests are appropriately managed and any complaints are satisfactorily resolved.

Residents and other service users are provided with guidelines based on this policy and understand that the policy is designed to protect and secure their personal information whilst ensuring that ECCT is able to share such information where it is necessary to safeguard the interests of the individual.

## 5. Application

Under the Act "personal data" is very widely defined as any personal information (including any opinion about the individual or images) that relates to an identifiable living person (whether in a personal or business capacity) which is stored electronically or held in a manual filing system. This policy therefore applies to every department and every location within ECCT and every individual about whom ECCT holds personal information and covers the use of CCTV.

All ECCT trustees, staff and volunteers are required to comply with this policy and procedures which outline ECCT's basic requirements on the collection, use, security, confidentiality, retention and disposal of personal data.

Executive Directors and Local Managers are responsible for ensuring compliance with the Act in their respective areas of responsibility.

All ECCT employees who have access to personal information are required to act in line with the Data Protection Act and any breach of this Policy or misuse of personal information by staff is misconduct which could result in action being taken in line with the Disciplinary Policy.

Residents, Friends, individual donors and third party suppliers and contractors have an understanding of the policy and how it applies to them.

Other agencies, regulators and partners are aware of the policy and acknowledge their role in implementing it.

## 6. Reason for the Policy

To ensure the Data Protection Act 1998 is complied with and that residents, staff, volunteers and other business partners are aware of ECCT's legal responsibilities under the Act, its organisational procedures for ensuring compliance and their individual rights under the Act.

## 7. What is new / What is different

This is a revision of a policy statement *Staff 9 Data Protection Act* last reviewed in December 2010. It has been fully reviewed and updated to cover all personal data collected and processed by the Trust, including residents, volunteers and other service users.

## 8. How to measure success

Signed Data Protection Policy Acknowledgement and Compliance Forms are held for all staff and volunteers.

Up to date training records are held for all members of staff whose job role is identified as involving access to personal data.

Complaints from individuals are systematically recorded and demonstrate compliance with the policy and legislations.

No enforcement action by the Information Commissioner's office, no reductions in regulatory framework ratings as a result of data protection breaches and no significant adverse media coverage.

## 9. Reference to relevant documents

Regulation / Guidance	In House Documents
Data Protection Act 2008	Freedom of Information Policy
Privacy & Electronic Communications	Complaints Management Policy

(EC Directive) Regulations 2003	
ICO- CCTV Code of Practice (2008)	Safeguarding Adults and Children at Risk Policy
ICO- Data Sharing Code of Practice	Whistleblowing Policy
ICO - Subject Access Code of Practice	Resident Involvement Policy
ICO - Employment Practices Code of Practice	Listening to our Customers Policy
ICO - Privacy Notices Code of Practice	Social Media Policy
ICO - Guide to Data Protection	Disposal of Redundant IT Policy
ICO - Direct Marketing	Recruitment for Location Staff and Head Office Policy
ICO - Guide to Privacy & Electronic Communications	Recruitment for Relief Bank Staff Policy
CQC – Essential Standards of Quality & Safety: Outcome Guidelines	Dignity, Privacy and Respect Policy
CQC – Code of Practice on Confidential Personal Data	Lettings Policy
Mental Capacity Act	Payroll Administration Policy*
	Training & Development Policy*
	Arrears Policy
	Information Security Policy*
	Email Policy*

All above Regulation & Guidance is available on the ICO's website: [www.ico.org.uk](http://www.ico.org.uk)

\* To be introduced

**10. Approval date** – September 2014

**11. Next review date** – September 2017

## **APPENDIX 1 - DEFINITIONS**

### **Consent**

Any freely given specific and informed indication of the individual's wishes by which the individual signifies their agreement to personal data relating to him/her being processed. Failure to respond / object should not be regarded as consent. Consent obtained under duress or on the basis of misleading information is not valid. Consent must be appropriate to the age and capacity of the individual and to the particular circumstances of the case. Consent may be withdrawn at a later date.

### **Data**

Information recorded in a way in which it can be processed by electronic equipment or through a structured manual filing system. This includes text and images eg CCTV recordings.

### **Data Controller**

A person / organisation who determines the purposes for which and the manner in which any personal data are, or are to be processed. Employees are not Data Controllers themselves, since they are exercising control of personal data on behalf of their employer, who ultimately has to take responsibility for their actions. The ExtraCare Charitable Trust is a data controller.

### **Data Processing**

Obtaining, recording or holding information; organising, amending or re-arranging data or extracting information from it, retrieving or using information, disclosing information by transmission, dissemination or making it available, erasure or destruction of the information.

### **Data Processor**

A person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller. This definition includes agents or contractors.

### **Data Subject**

An individual who is the subject of personal data, for example an employee, resident, volunteer etc.

### **Explicit Consent**

This is one of the conditions for processing sensitive personal data and must be absolutely clear and requires the individual to consent to the specific processing, the specific type of data, the purposes of the processing and any sharing.

### **Notification**

The Information Commissioner's Office maintains a public register of data controllers. Each register entry includes the name and address of the data controller

and details about the types of personal data they process. Notification is the process by which a data controller's details are added to the register.

### **Personal Data**

Data, which relates to an individual who can be identified from it, either by name or code e.g. employee number. Also included are any expression of opinion about the person and any indication of the intentions of the Data Controller in respect of the individual.

### **Privacy Notice**

The first principle of the Data Protection Act is that data must be processed lawfully and fairly and this means that certain information must be given to individuals when data is collected. The oral or written statement that individuals are given when information about them is collected is often called a "*fair processing notice*" or a "*privacy notice*". The Privacy Notice should state the identity of the organisation collecting the data, the purpose for which the information will be used and any relevant information for example on data sharing.

### **Sensitive Personal Data**

includes:

Racial or ethnic origin

Political opinions

Religious or other beliefs

Physical or mental health or condition

Sex life

Criminal convictions/proceedings

Trade union membership

### **Subject access request (SAR)**

Under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records, by writing to the person or organisation they believe holds it. A subject access request must be made in writing (email is acceptable) and must be accompanied by the appropriate fee, usually up to a maximum of £10. Once the applicable fee has been paid, a reply must be received within 40 calendar days.

## APPENDIX 2 – ICO NOTIFICATION



# Data Protection Register - Entry Details

---

**Registration Number: Z5300341**

**Date Registered: 25 May 2001 Registration Expires: 24 May 2015**

**Data Controller: THE EXTRA CARE CHARITABLE TRUST**

**Address:**

7 HARRY WESTON ROAD  
BINLEY BUSINESS PARK  
BINLEY  
COVENTRY  
CV3 2SN

---

**This register entry describes, in very general terms, the personal data being processed by:**

THE EXTRA CARE CHARITABLE TRUST

**Nature of work - Charity (National)**

**Description of processing**

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

**Reasons/purposes for processing information**

We process personal information to enable us to provide a voluntary service for the benefit of the national public as specified in our constitution; administer membership records; to fundraise and promote the interests of the charity; manage our employees and volunteers; maintain our own accounts and records. Our processing also includes the use of CCTV systems for the prevention of crime.

## **Type/classes of information processed**

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- lifestyle and social circumstances
- suppliers and service provider details
- financial details
- education and employment details
- visual images, personal appearance and behaviour
- complaints and enquiries
- health, safety and security details

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature
- offences and alleged offences
- criminal proceedings, outcomes and sentences
- trade union membership
- sexual life

## **Who the information is processed about**

We process personal information about:

- staff
- volunteers
- supporters
- tenants
- clients/customers
- complainants and enquirers
- representatives of other organisations
- individuals captured by CCTV images
- applicants for accommodation which include families and household
- landlords
- local authority employees
- probation officers
- social workers
- spiritual and welfare advisers
- consultants and professional advisers
- suppliers and service providers
- survey respondents
- offenders and suspected offenders

## **Who the information may be shared with**

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of

the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- family, associates or representatives of the person whose personal data we are processing
- employees
- current, past and prospective employers
- healthcare, social and welfare organisations
- providers of goods and services
- educator and examining bodies
- financial organisations
- employment and recruitment agencies
- survey and research organisations
- business associates and professional advisers
- police forces
- local and central government
- other companies in the same group as the data controller
- other voluntary and charitable organisations
- auditors
- other housing associations or trusts
- health authorities
- enquirers and complainants
- credit reference agencies
- debt collection and tracing agencies

### **Transfers**

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the data protection act.

Copyright in this copy is owned by the Information Commissioner. Data Controllers may take copies of their own register entries. Apart from that no part of it may be copied unless allowed under the Copyright Designs and Patent Act 1988.

---

[© Copyright](#)

### **APPENDIX 3 – DATA PROTECTION PRINCIPLES**

The 1998 Act defines eight principles covering the way in which personal data must be processed.

1. Personal information must be fairly and lawfully processed and, in particular, shall not be processed unless specified conditions are met (see Appendix 4)
2. Personal information must be processed for specified limited purposes.
3. Personal information must be adequate, relevant and not excessive.
4. Personal information must be accurate and up to date.
5. Personal information must not be kept for longer than necessary.
6. Personal information must be processed in line with data subjects' rights.
7. Personal information must be secure.
8. Personal information must not be transferred to a country or territory outside the European Economic Area without adequate protection.

**APPENDIX 4 – LAWFUL CONDITIONS FOR PROCESSING DATA**

Personal data **MUST NOT** be processed unless one of the following conditions is met:-

1. The data subject has given his consent to the processing.
2. The processing is necessary—
  - a. for the performance of a contract to which the data subject is a party (eg an employment contract, tenancy / leasehold, care contract etc), or
  - b. for the taking of steps at the request of the data subject with a view to entering into a contract (eg recruitment, applications for services)
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract (ie to comply with any legislative requirement)
4. The processing is necessary in order to protect the vital interests of the data subject (ie safeguarding)
5. The processing is necessary for the administration of justice or for exercising statutory, governmental or other public functions.
6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, **except** where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

**Sensitive** personal data (including health / medical conditions) **MUST NOT** be processed unless one of the above conditions is met **AND at least one of the following conditions** is met:-

1. The data subject has given explicit consent to the processing
2. The processing is necessary to comply with employment law
3. The processing is necessary to protect the vital interests of:-
  - a. The individual (where consent can not be given or reasonably obtained); or

- b. Another person (where the individual's consent has been unreasonably withheld)
4. The individual has deliberately made the information public
5. The processing is necessary in relation to legal proceedings., for obtaining legal advice or otherwise for establishing, exercising or defending legal rights
6. The processing is necessary for administering justice or exercising statutory or governmental functions
7. The processing is necessary for medical purposes and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
8. The processing is necessary for anti-fraud purposes.

## **APPENDIX 5 - CCTV**

Images of people are covered by the Data Protection Act, and so is information about people which is derived from images – for example, vehicle registration numbers. CCTV is covered by the Act where they are capturing images. Dummy or out of order cameras are not covered.

The Data Protection Act does not apply to individuals' private or household purposes. So if residents or their families install cameras in their own apartments, the Act will not apply. Also images captured for recreational purposes, such as with a mobile phone, digital camera or camcorder, are also exempt.

### **Purpose of CCTV at ECCT**

EECT uses CCTV at its locations [and in its shops] for the monitoring and collection of visual images for the purpose of maintaining the security of the premises, for the prevention of crime, its detection and investigation and for the apprehension and prosecution of offenders

### **Location of CCTV**

This purpose governs where cameras are located eg area vulnerable to crime or areas designed to protect the security of premises; car parks and entrances & exits.

### **Signage**

Where a site is covered by operational CCTV, there must be clear and prominent signs at the entrance to the area covered by CCTV and within the areas as well stating who operates the CCTV, the purpose for using CCTV and who to contact about the scheme.

In the exceptional circumstance that audio recording is being used, this should be stated explicitly and prominently.

All staff should know what to do or who to contact if someone makes an enquiry about the CCTV.

### **Data Protection Measures**

The same principles apply to CCTV images as to personal files. Procedures on data security, sharing & Data subject access requests all apply to CCTV images.

Further information is available from the Company Secretary and in the ICO's CCTV Code of Practice.