Policy Name	Data Protection
Version No.	2.0
Approval Date	Dec 2017
Category	Corporate
Classification	Internal

Data Protection

Author	Governance & Risk Officer
Contributors	Company Secretary, Head of Assurance, Head of IT, Head of HR Services, Head of Finance, Head of Sales, Training & Development Manager
Review Frequency	3 years
Latest Review Date	December 2017
Approved By & Date	Board - 11 December 2017
Next Review Date	December 2020

Contents

Policy Name	Data Protection
Version No.	2.0
Approval Date	Dec 2017
Category	Corporate
Classification	Internal

Version Control

Version	Date	Description	Updated By	Approved By
0.1	Sept 17	1st draft (new version)	Sue Allred	Vikki Hall
0.2	Oct 17	2nd draft (inc comments)	Sue Allred	Vikki Hall
2.0	Nov 2017	Approved draft policy	Vikki Hall	ELT, Audit & Assurance Committee
2.0	Dec 2017	Approved policy (no changes)	Vikki Hall	Board of Trustees

1. Policy Purpose & Aim

The ExtraCare Charitable Trust (ECCT) needs to gather and use certain information about individuals, including for example, residents, suppliers, volunteers, employees, donors and supporters and other people we have a relationship with or may need to contact.

This policy aims to protect the privacy of and promote the rights of individuals whose personal and confidential information is held by ECCT. ECCT will ensure that it has the necessary information to deliver its mission, to manage its employees and volunteers and to engage with other individuals in delivering its charitable objectives.

This policy describes how this personal data must be collected, handled and stored to meet ECCT's data protection standards and to comply with the law.

A Glossary of Terms used within this policy is included at Appendix A.

2. Objectives

The objectives of this policy are to:

- Ensure that data protection is considered as part of every business decision and is managed as an integral part of ECCT's activities.
- Protect and secure an individual's information whilst ensuring that information can be shared appropriately to meet legitimate business and safeguarding needs.
- Meet the requirements of all legislative and regulatory guidelines in order to minimise the risk of enforcement action by regulatory bodies and diminution of reputation.
- Develop employees' and volunteers understanding of data protection through training and awareness so that data protection becomes embedded in ECCT's culture.

3. Scope of Policy

This policy applies to all information that ECCT holds relating to an identified or identifiable natural person (data subject). An identifiable natural person is a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The policy applies to all forms in which the personal information is held, whether in hard copy or electronic form.

All ECCT Trustees, staff, volunteers and contractors 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 information.

4. Responsibilities

The Board of Trustees is ultimately responsible for ensuring ECCT meets its legal obligations including in relation to data protection and is responsible for approving this policy.

The Executive Leadership Team is responsible for ensuring this policy is appropriately implemented across ECCT and is embedded into ECCT culture.

ECCT Managers are responsible for ensuring compliance with this policy in their respective areas of responsibility.

All ECCT employees must participate in the mandatory training on information security, data protection and cyber security.

Every employee, volunteer or contractor who has access to personal information held by ECCT must ensure it is kept secure and confidential at all times and is only used for the purpose(s) for which it was collected.

Every employee, volunteer, contractor who has access to personal information held by ECCT is responsible for complying with this policy and other ECCT policies which are relevant to data protection. Any breach of this policy or misuse of personal information by employees is misconduct which could result in action being taken in line with the Disciplinary Policy.

The following roles have the following specific responsibilities:

Executive Director – Corporate Resources

- To approve directed covert surveillance as set out in the CCTV Policy.
- To act as ELT Lead on data protection breaches as set out in the Information Security Policy.

Head of IT

- To ensure robust arrangements are in place to implement and maintain appropriate technical measures to protect personal information held on ECCT's network and devices, including the ability to:

- ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
- restore the availability and access to personal information in a timely manner in the event of a physical or technical incident according to the specified back up cycle, retention periods and to agreed SLAs.

- To implement and carry out vulnerability and penetration testing as required and ensure that new measures are evaluated as appropriate before implementation.
- To evaluate any third party services that ECCT is considering using to store or process data, e.g. cloud computing services.

Company Secretary

ECCT has appointed the Company Secretary as its Data Protection Officer with the following statutory responsibilities:

- To inform and advise ECCT and its employees about their obligations to comply with the data protection laws.
- To monitor compliance with data protection in ECCT.
- To be the first point of contact for the Information Commissioner's Officer (ICO) and other supervisory authorities and for individuals whose data is processed (employees, customers etc).

In addition, the Company Secretary will be responsible for ensuring that any regulatory requirements in relation to registration with or notification to the ICO are met and will be supported by the Governance and Risk Officer.

In fulfilling these responsibilities, the Company Secretary will operate independently of management and report directly to the Board of Trustees.

5. Monitoring & Review

ECCT is committed to ensuring that all appropriate technical and organisational measures are taken against unauthorised or unlawful processing of data and against accidental loss or destruction of or damage to personal data.

ECCT will monitor the effectiveness of this policy through the utilisation of existing business as usual monitoring, scrutiny and oversight processes and through the ongoing review of breach reporting. Lessons learned from data protection breaches or near misses will be implemented through revisions to Work Instructions and training.

ECCT will conduct a fundamental review of this policy at least every three years taking into account legislative and regulatory changes.

6. Risk Management

The Board of Trustees have identified a breach of legislative and regulatory requirement as a corporate risk, for which they have a low tolerance (appetite). A breach of the Data Protection Act represents a financial and reputational risk for the Trust. Compliance with this policy and related documents reduces the risk of a breach and ensures that the Trust meets its legislative and regulatory obligations.

7. Statement of Commitment

7.1. 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. ECCT acknowledges that all individuals have the right to expect that appropriate safeguards will be operated to protect the confidentiality and integrity of their personal data or information.

7.2. ECCT will ensure that it allocates appropriate resources to data protection including, without limitation, by providing the Data Protection Officer, supported by the Governance and Risk Officer, with the resources necessary to carry out their tasks. This will include access to appropriate technical training to develop and maintain their expert knowledge.

7.3. ECCT will document what personal information it holds, where it came from and with whom it is shared.

7.4. Where ECCT relies on an individual's consent to process personal information it will ensure that consent is freely given, specific and informed. Requests for consent will be clear, prominent and require an unambiguous and clear affirmative indication signifying agreement. When requesting consent, ECCT will advise individuals of the right to withdraw consent and ECCT will not make consent a condition of a contract. ECCT will keep records of consent.

7.5. ECCT will ensure that all staff are trained to handle personal information appropriately and receive mandatory data protection training, as part of Information Security awareness. ECCT will also promote the Data Protection Policy and Records Management Policy (relating to

storage, retention and disposal of personal information records) to staff, residents, volunteers, and suppliers/ contractors.

7.6. ECCT will develop and publish Work Instructions providing detailed procedures for staff and volunteers on how to apply and implement this policy. These will be kept under review and revised as necessary to ensure they are effective.

7.7. ECCT will meet the following data protection principles:

Personal information will be processed lawfully, fairly and in a transparent manner in relation to individuals;	1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes	Personal information will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Personal information will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;	3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date	Personal information will be accurate and, where necessary, kept up to date; having regard to the purposes for which the personal information is processed, every reasonable step will be taken to ensure that personal information which is inaccurate is erased or rectified without delay;

Personal information will be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal information is processed.

5. Personal information must not be kept for longer than is necessary

6. Personal information must be secure

Personal information will be processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7.8. ECCT will establish a framework to demonstrate how it meets the data protection principles and implements this policy.

7.9. ECCT will adopt a privacy by design approach to all projects to promote privacy and data protection compliance from the start. At the start of any project and throughout its lifecycle ECCT will undertake a Privacy Impact Assessment (PIA), especially for the following:

- building new IT systems for storing or accessing personal data;
- developing policies or strategies that have privacy implications;
- embarking on data sharing initiatives; or
- using data for new purposes.

7.10. ECCT will provide individuals with all relevant information that they require to understand and exercise their rights under Data Protection legislation. This is set out in ECCT's Privacy Policy available on www.extracare.org.uk

7.11. ECCT will only share personal data in accordance with the requirements of any legislation, taking into account regulatory guidance and will inform individuals of the identity of other parties to whom we may disclose or be required to provide personal data, the circumstances in which this may happen and when any exceptions to this rule may apply.

7.12. Where ECCT appoints a third party to process personal information on its behalf, ECCT will ensure that the relationship is governed by a binding contractual relationship and that the processor undertakes to process the information only in accordance with documented instructions from ECCT, keep the information secure and confidential.

7.13. Where ECCT needs to transfer personal information outside the European Economic Area (EEA), prior to doing so it will ensure that the party and country to whom the personal information is being transferred can provide the same level of protection as provided by data protection laws in the EEA.

7.14. Deliberately obtaining or disclosing personal data unlawfully is an offence and ECCT will report any such incidents to the appropriate authorities. ECCT may consider taking internal disciplinary action in line with ECCTs Disciplinary Policy where staff do not comply with data protection legislation, ECCT policies or the accompanying Work Instructions.

8. Breach Reporting

ECCT recognises that no organisation handling personal information can guarantee it will never experience breaches but that residents and staff have a right to expect that ECCT achieve and maintain high standards in this important area.

ECCT acknowledges the importance of transparency and accountability in managing personal information.

ECCT requires every data breach or near miss to be captured to ensure that lessons are learned. As an organisation ECCT is wholly dependent on each and every employee playing their part, accepting their personal responsibility and holding each other to account.

Employees are required to report all information security breaches including data protection breaches, without delay, as set out in the Information Security Policy.

ECCT has set up a dedicated email address for the reporting of data protection breaches. databreach@extracare.org.uk

All data protection breaches will be logged and handled in accordance with the procedures set out in the Information Security Policy.

With effect from 25 May 2018, ECCT will have a statutory obligation to report personal data breaches to the Information Commissioner's Office within 72 hours, and, in certain cases, to make individuals aware that their personal information has been compromised. ECCT is committed to identifying and reporting breaches within this timescale and will ensure that all staff are made aware of this.

9. Other Relevant ECCT Policies & Documents

Policies	• Information Security Policy • Records Management Policy • Information Classification Policy • Freedom of Information Policy • Complaints Management Policy • CCTV Policy* • Safeguarding Adults and Children at Risk Policy • Whistleblowing Policy • Resident Involvement Policy • Social Media Policy • Disposal of Redundant IT Equipment Policy • Recruitment of Location & Head Office Staff • Recruitment for Relief Bank Staff Policy • Dignity, Privacy & Respect Policy • Lettings Policy • Payroll Administration Policy • Training & Development Policy • Income Management Policy • Use of Email Policy • Privacy Policy (website) • New Village Sales Policy • Resales Policy • Disciplinary Policy • Grievance Policy
Work Instructions	• Collection, Use & Sharing • Data Subject Access Request • Privacy Impact Assessment
Other	• Staff Handbook • Employment Contract • Information Security Training e-workshop (all staff)

10. Relevant Legislative & Regulatory Requirements

Legislation	Regulation	Guidance
Data Protection Act 1998 (until 24 May 2018)		ICO – CCTV Code of Practice (2017)
General Data Protection Regulation 2016 (from 25 May 2018)		ICO – Data Sharing Code of Practice

Data Protection Bill 2017		ICO – Subject Access Code of Practice
Privacy & Electronic Communications (EC Directive) Regulations 2003		ICO – Guide to data protection
Mental Capacity Act		ICO – Direct Marketing
Care Act 2014		ICO – Guide to Privacy & Electronic Communication
Human Rights Act 1998		CQC – Code of Practice on Confidential Personal Data
Regulation of Investigatory Powers Act 2000;		Surveillance Camera Code of Practice (Home Office June 2013)
		National Housing Federation Code of Practice

Appendix 1 – Glossary of Terms

Data

Data is information that is processed electronically i.e. on a computer, including word processing documents, emails, computer records, CCTV images, archived files or databases, faxes and information recorded on telephone logging systems.

Data is also information held manually or 'hard copy' files which are structured, (filed by subject, reference, dividers or content) and where individuals can be identified and information easily accessed without the need for excessive searching.

Data is also information forming part of a manual medical, housing and/or social care record.

Personal Data

'Personal data' is defined as any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical or physiological, genetic, mental, economic, cultural or social identity natural person.

Special Categories of Personal Data

Any personal data (above) but which contains information relating to race, political opinion, religious belief, trade union membership, physical or mental health, sex life and unique identity of a person by processing biometric or genetic data.

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 Controller

For the purpose of this policy it relates to ECCT who determines the purpose and manner in which personal data is processed

Data Processor

A person other than an employee of the data controller who process personal data on behalf of the data controller – usually a contractor

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

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 them 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 by the individual at any time.

Explicit consent

This is one of the conditions of processing special categories of 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.

Privacy notice

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, any relevant information on who the data will be shared with, how long the information will be kept for and the rights of the data subject.

Subject access requests (SAR)

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). A reply must be provided within 30 calendar days.