| | |
|---|---|
| Policy Name | Data Protection Policy |
| Version No. | 2.1 |
| Approval Date | October 2020 |
| Category | Corporate |
| Classification | Internal |

# Data Protection Policy

| | |
|---|---|
| Author | Governance & Risk Officer |
| Contributors | Company Secretary, Legal Officer, Head of Assurance, Head of IT, Head of People, Head of Finance, Head of Sales and Payroll, Payroll and Learning and Development Manager. |
| Review Frequency | 3 years |
| Latest Review Date | October 2020 |
| Approved By & Date | ELT November 2020, Audit & Assurance Committee November 2020 |
| Next Review Date | **October 2023** |

**Contents**

| | |
|---|---|
| Policy Name | Data Protection Policy |
| Version No. | 2.1 |
| Approval Date | October 2020 |
| 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 (including 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 |
| 2.1 | Oct 2020 | Updated following review | Vanita Ruparel | Chris Skelton |

| | |
|---|---|
| Policy Name | Data Protection Policy |
| Version No. | 2.1 |
| Approval Date | October 2020 |
| Category | Corporate |
| Classification | Internal |

## 1. Policy Purpose & Aim

The ExtraCare Charitable Trust (ExtraCare) is a 'Data Controller' for the purposes of data protection legislation and to carry out our business functions effectively, we need to gather and use certain information about individuals, including for example, residents, suppliers, volunteers, staff members, donors and supporters and other people we have a relationship with or may need to contact.

This policy:

- Outlines ExtraCare's core requirements on the collection, use, security, confidentiality, retention and disposal of personal data and aims to protect the privacy of and promote the rights of individuals whose personal data is held and/ or shared by ExtraCare;
- Describes how the Personal Data used by ExtraCare is to be collected, handled and stored to meet ExtraCare's data protection standards and to comply with the law;
- Serves as our principal 'Appropriate Policy Document' as required under data protection legislation in connection with certain data which is defined in law as more sensitive ("special category data") as set out at section 7 below; and
- Forms part of our framework of technical and other measures which help us to discharge our responsibilities under data protection law and other regulatory requirements.

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 ExtraCare's activities;
- Protect and secure an individual's information whilst ensuring that information can be used and shared appropriately to meet ExtraCare's 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; and
- Develop employees' and volunteers understanding of data protection (which is also achieved through training and awareness) so that data protection becomes embedded in ExtraCare's culture.

## 3. Scope of Policy

This policy applies to all Personal Data that is held by ExtraCare or ExtraCare's group companies relating to an identified or 'identifiable natural person' (data subject).

The people we generally hold information about are:

- Prospective, current and past employees and contractors;
- Prospective, current and past residents;
- Prospective, current and past volunteers;
- Users of the village/scheme facilities (e.g. friends of the village, gym members, class users) and
- Donors

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

This policy also applies where the data is processed by third parties on behalf of ExtraCare.

## 4. Responsibilities

The Board of Trustees is ultimately responsible for ensuring ExtraCare 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 ExtraCare and is embedded into ExtraCare culture.

ExtraCare Managers are responsible for ensuring compliance with this policy in their respective areas of responsibility and they must ensure approval is obtained from the IT team and the Data Protection Officer of any new IT service or system which is to process and/or store personal data prior to any IT service or system being purchased.

Every employee, volunteer or contractor who has access to personal data used by ExtraCare must ensure it is kept secure and confidential at all times and is only used in accordance with this policy. In addition, every employee is required to complete mandatory training provided by the company.

Every employee, volunteer and contractor who has access to personal data held by ExtraCare is responsible for complying with this policy and other ExtraCare policies which are relevant to data protection (as set out in section 7 below).

We wish to emphasise that deliberately obtaining or disclosing personal data unlawfully is an offence and ExtraCare may report any such incidents to the appropriate authorities. ExtraCare may also consider taking internal disciplinary action in line with ExtraCare's Disciplinary Policy where

staff do not comply with data protection legislation, ExtraCare policies or the accompanying Work Instructions.

The following roles have the following specific responsibilities:

**Executive Director – Corporate Resources**

- To act as ELT Lead on Personal Data breaches;
- To approve directed covert surveillance as set out in the CCTV Policy.

**Head of IT**

- To ensure robust arrangements are in place to implement and maintain appropriate technical measures to protect personal information held on ExtraCare's MPLS 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 information within the Citrix environment (excluding SaaS applications accessed from within Citrix) 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 penetration testing as required and ensure that new measures are evaluated as appropriate before implementation.
- To evaluate any third party services that ExtraCare are considering using to store or process data, e.g. cloud computing services.

**Data Protection Officer (DPO)**

Requirements:

- The GDPR says that a DPO should be appointed on the basis of their professional qualities, and in particular, experience and expert knowledge of data protection law.
- As the personal data processed by ExtraCare is particularly complex and/ or risky, the knowledge and abilities of the DPO should be correspondingly advanced enough to provide effective oversight.

ExtraCare has appointed the Director of Governance & Compliance as Company Secretary and Data Protection Officer (DPO). The postholder of DPO will have the following statutory responsibilities:

- To inform and advise ExtraCare and its employees about their obligations to comply with the Data Protection law;
- To monitor compliance with data protection in ExtraCare;

- To provide advice regarding Data Protection Impact Assessments (DPIAs) and other legal assessments under Data Protection law;
- To put in place all appropriate Data Protection Agreements with any third party Personal Data is shared with; and
- To be the first point of contact for the Information Commissioner's Office (ICO), other supervisory authorities and for individuals whose data is processed (employees, customers etc).

In addition, the DPO 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 Team.

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

**Data Protection Queries and what to do should the DPO be unavailable**

Any privacy or data protection questions which are not directed to the above roles specifically (or in the event that the DPO is unavailable) should be directed to the Data Protection email account of privacy@extracare.org.uk, which is managed by the Governance Team. Should it be necessary to appoint an Interim DPO, this appointment will be made by ELT.

## 5. Monitoring & Review

ExtraCare 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.

ExtraCare 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.

ExtraCare 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 data protection law represents a financial and reputational risk for ExtraCare. 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, the 7 Data Protection Principles and ExtraCare's approach

ExtraCare 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. ExtraCare 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.

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

The **7 Data Protection Principles** set out in data protection legislation require personal data to be:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency);
- Collected only for specified, explicit and legitimate purposes, and not further processed in a way which is incompatible with those purposes (Purpose limitation);
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data minimisation);
- Accurate and where necessary kept up to date (Accuracy);
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage limitation);
- Processed in a way that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality); and
- ExtraCare is responsible for and must be able to demonstrate documentary evidence portraying our compliance with each of the data protection principles listed above (Accountability).

In order to comply with the above, we set out below in general terms, how ExtraCare approaches each of these principles:

**Processing and Use of Personal Data**

ExtraCare will maintain a general record of processing in accordance with data protection legislation, setting out what personal information it holds, where it came from and with whom it is shared.

We generally rely on the following lawful bases for processing personal data:

- The processing is necessary to perform a contract with the data subject (for instance, the contracts with our residents or employment contracts with our staff).
- The processing is necessary to comply with our legal obligations, including our Charitable Objects and regulatory requirements parts of our business and activities are subject to.
- The processing is necessary for the purposes of legitimate interests pursued by ExtraCare, balanced with the privacy rights of the individuals whose data we are processing. We have identified that we have legitimate interests in growing and managing our charity effectively and efficiently and ensuring that the rights and interests of our residents and staff are protected and promoted.

We do not normally rely on consent as our general basis of processing personal data. Where ExtraCare relies on an individual's consent to process personal information it will ensure that consent is freely given, specific and informed. When requesting consent, ExtraCare will advise individuals of the right to withdraw consent and ExtraCare will not make consent a condition of a contract. ExtraCare will keep records of consent. These will be stored on systems/in locations managed by the team or department to which the consent to processing relates and should be accessible for review by the DPO.

We process certain special category data in connection with our functions as a charity, business and employer and to perform certain regulatory obligations. In general terms, the legal bases for such processing is:

- It is necessary for the purposes of performing or exercising obligations or rights of ExtraCare or the data subject for the purposes of employment, social security or 'social protection';
- It is necessary to protect an individual's vital interests;
- It is necessary for the purposes of promoting and maintaining equality of opportunity or treatment by ExtraCare;
- It is necessary for safeguarding purposes, the prevention or detection of unlawful acts, or the provision of support services;

- It is necessary for establishing, exercising and defending legal rights.

We will have regard to the ICO's Code of Practice on Direct Marketing in determining our approach. We will respect people's choices not to receive direct marketing from us. We will not use 'bought in' lists of potential targets unless the respective individuals on the lists have consented to their data being shared with ExtraCare for the relevant purpose beforehand and will ensure we have either specific consent, or that we can rely on the 'soft opt in' for any electronic marketing communications we send to customers or potential customers.

**Fairness and Transparency**

General information about how we process personal data (sometimes known as "fair processing information") will be available in our Privacy Policy on www.extracare.org.uk. In some circumstances, we may make further, specific privacy information available to people whose data may be processed – for instance, notices of CCTV usage. Please see the CCTV Policy for more information.

We will normally provide fair processing information at the time we collect the personal data. We recognise that in certain circumstances it may not be possible or appropriate to provide fair processing information at that time, and we therefore will ensure that our general privacy notices are widely available. We will not provide fair processing information where to do so would undermine the prevention or detection of crime or adversely affect our ability to exercise or defend our legal rights.

We will take all reasonable steps to tell people if we are recording telephone calls with us.

Responsibility for maintaining the privacy notices sits with the Governance Team.

**Data Minimisation**

We will process personal data in a way that is adequate, relevant and limited to what is necessary for our purposes. This means that all personal data must be handled through corporate systems. We will undertake back-ups of our systems and emails (sent and received) for business continuity purposes.

Unnecessary copies of information must be deleted or securely destroyed.

Staff and contractors must only process personal data as required to carry out their role. We may monitor or audit the use of data to ensure that this happens. We will limit through 'role-based access' our systems based on the data an employee is reasonably likely to need to access to perform their role. The IT Department or the relevant business owner (depending on the software/ system) are responsible for implementing these controls. Further access may be granted (or restricted) on a case-by-case basis with managers', HR, Governance Team and IT involvement.

**Accuracy**

We will ensure as far as possible that the data we hold is accurate and kept up to date. Staff and contractors are responsible for checking the accuracy of any personal data when they collect it. Staff and contractors must take all reasonable steps to destroy or update inaccurate personal data as far as permitted by law.

**Storage limitation, retention and destruction**

We will ensure that personal data is not kept in an identifiable form for longer than is necessary. Details of our retention and disposal periods are set out in our Records Management Policy. Staff and contractors are responsible for storing personal data in accordance with this policy.

**Security, integrity and confidentiality**

We will develop, implement and maintain appropriate data security systems and specific policies to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

We will regularly review, evaluate and test the effectiveness of our data security systems.

Staff must comply with the above-mentioned policies including, but not limited to: the Information Security Policy, Homeworking Policy, IT Security Policy, Acceptable Use Policy, Information Classification Policy, Social Media Policy and Record Management Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain for security purposes.

ExtraCare will ensure that all staff are trained to handle personal information appropriately and receive mandatory data protection, information security and cyber security training, as part of Information Security awareness.

ExtraCare 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.

**Data protection by design and default, project development and Data Protection Impact Assessments**

ExtraCare will adopt a 'data protection by design and default' approach to all projects to promote data protection compliance from the start. At the start of any project and throughout its lifecycle ExtraCare staff are to consider whether a Data Protection Impact Assessment (DPIA) should be undertaken, 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.

Employees and contractors should refer to the Data protection Impact Assessment Work Instruction for guidance on how this is to be carried out.

Advice on any DPIA will be given by the Data Protection Officer and records of the DPIA will be stored by the Governance Team.

Where any new use of CCTV, staff or customer monitoring or surveillance technologies are being considered, a DPIA should be carried out.

**Automated processing and decision making**

Generally, we do not engage in automated processing/profiling, or automated decision-making (i.e. significant decisions about a person made solely by a computer without any human control).

**Data Processors**

We may contract with other organisations to process personal data on our behalf, either specifically or as part of broader services they provide for ExtraCare. We will only appoint a data processor if, having carried out due diligence, we are satisfied that they can implement appropriate technical and organisational measures that meet the requirements of the data protection legislation. The appointment of a data processor must include the contractual requirements specified in data protection legislation, and in particular, we 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 ExtraCare, keep the information secure and confidential. All employees and contractors are required to email privacy@extracare.org.uk to notify the Governance Team of any new or existing supplier which will be processing personal data to ensure the appropriate Data Processing Agreement can be put in place.

**International data transfers**

We are a charity primarily operating in the UK and from a governance perspective we prefer for our data to be held in the UK. From time to time we may need or want to transfer personal information to third countries, including because of a choice of supplier that we use. Prior to transferring any data internationally, we 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 UK.

**Individuals' rights**

ExtraCare 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 ExtraCare's Privacy Policy available on www.extracare.org.uk, accessible versions of the information can be made available on request.

Whilst we recognise that under data protection law individuals can exercise their rights verbally, we encourage individuals to make their request in writing to ensure there is an audit trail.

Individuals have a right to request access to their personal data held by ExtraCare. individuals should refer to the Subject Access Request (SAR) Work Instruction for further information on how such a request can be made and how it is to be processed. Any member of staff, volunteer or contractor who receives a request from a data subject to exercise their SAR rights must send the request on to privacy@extracare.org.uk immediately.

**Data sharing**

ExtraCare will only share personal data in accordance with the requirements of any legislation, taking into account regulatory guidance. We 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.

## 8. Breach Reporting

**What is a Personal Data Breach?**

The statutory definition of a personal data breach is: a breach of security, leading to the accidental or unlawful destruction, loss, alteration, unauthorised, disclosure of or access to, personal data, transmitted, stored or otherwise processed by ExtraCare.

ExtraCare requires every personal data breach to be captured and recorded to ensure that lessons are learned and that we can comply with our obligations under data protection law. As an organisation ExtraCare 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 personal data breaches, without delay to databreach@extracare.org.uk.

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

ExtraCare has a statutory obligation to report personal data breaches where there is a likely risk to the rights and freedoms of individuals to the Information Commissioner's Office within 72 hours, and, in certain cases, to make individuals aware that a breach may pose a significant risk to them. ExtraCare is committed to identifying and reporting necessary breaches within this timescale and will ensure that all staff are made aware of this. A Data Breach Assessment will be completed by the Governance Team once a breach has been reported to determine whether the breach should be reported to the ICO and/or whether affected individuals should be notified (all decisions should be documented accordingly). Any breach which is identified to be reported to the ICO, will first be reviewed by the Data Protection Officer and Legal Officer who will consult with necessary ELT

members before reporting the breach to the ICO (ensuring the Board of Trustees are made aware as and when necessary).

## 9. Other Relevant ExtraCare Policies & Documents

| | |
|---|---|
| Policies | Information Security Policy<br>Records Management Policy<br>Information Classification Policy<br>Complaints Management Policy<br>CCTV Policy*<br>Safeguarding Adults and Children at Risk Policy<br>Whistleblowing Policy<br>Customer Engagement Policy<br>Social Media Policy<br><br>Recruitment of Location & Head Office Staff<br>Recruitment for Relief Bank Staff Policy<br>Dignity, Privacy & Respect Policy<br>Lettings Policy<br><br>Training & Development Policy<br>Income Management Policy<br>IT Security Policy<br>Privacy Policy (website)<br>New Village Sales Policy<br>Resales Policy |

| | |
|---|---|
| | Disciplinary Policy<br>Grievance Policy |
| Work Instructions | Collection, Use & Sharing data<br>Subject Access Request<br>Data Protection Impact Assessment<br>Use of Email |
| Other | Staff Handbook<br>Employment Contract<br>Information Security Training e-workshop (all staff)<br>Cyber Security eLearning (All staff) |

## 10. Relevant Legislative & Regulatory Requirements

| Legislation | Regulation | Guidance |
|---|---|---|
| Data Protection Act 2018 | | ICO – CCTV Code of Practice (2017) |
| General Data Protection Regulation and successor UK legislation | | ICO – Data Sharing Code of Practice |
| | | 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 |
| | | 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 ExtraCare who determines the purpose and manner in which personal data is processed.

**Data Processor**

A third party which processes personal data on behalf of the data controller under the sole and specific instructions of the Data Controller.

**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 reply must be provided within 30 calendar days.