| | |
|---|---|
| Policy Name | Data Protection Policy |
| Version No. | 3 |
| Approval Date | May 2022 |
| Category | Corporate |
| Classification | Internal |

# Data Protection Policy

| | |
|---|---|
| Author | Compliance and Risk Manager |
| Contributors | Legal Manager; Corporate Projects Co-ordination Manager, SMT |
| Review Frequency | 3 years |
| Latest Review Date | May 2022 |
| Approved By & Date | Audit & Assurance Committee and Board (May 2022) |
| Next Review Date | May 2025 |

**Contents**

| | |
|---|---|
| Policy Name | Data Protection Policy |
| Version No. | 3 |
| Approval Date | May 2022 |
| Category | Corporate |
| Classification | Internal |

**Version Control**

| Version | Date | Description | Updated By | Approved By |
|---|---|---|---|---|
| 1.0 | Nov 2017 | First draft | Governance and Risk Officer | ELT, Audit and Assurance Committee |
| 2.0 | Dec 2017 | Approved Policy | Company Secretary | Board of Trustees |
| 2.1 | Dec 2020 | Updated following review | Legal Manager | Board of Trustees |
| 3.0 | May 2022 | Transferred to updated template. Policy made more concise, detail included in work instructions, responsibilities updated | Compliance and Risk Manager | ELT, Audit and Assurance Committee |
| 3.0 | May 2022 | Approved Policy | Compliance & Risk Manager | Board of Trustees |

| Policy Name | Data Protection Policy |
|---|---|
| Version No. | 3 |
| Approval Date | May 2022 |
| Category | Corporate |
| Classification | Internal |

## 1. Policy Purpose & Aim

1.1 This policy outlines ExtraCare's approach to Data Protection. We recognise the importance of protecting the personal data we are entrusted with, and complying with relevant legislation including:

- The UK General Data Protection Regulation (UK GDPR);
- The Data Protection Act 2018 (DPA 2018);
- The Privacy and Electronic Communications Regulations (2003) (PECR);
- The Computer Misuse Act 1990 (CMA);
- The common law duty of confidentiality; and
- Any other laws and regulations relating to the protection of personal data.

1.2 We need to process personal information about residents, customers, and employees to operate. It is in everyone's interests to handle data sensitively and appropriately and we are trusted by residents, customers, and colleagues to do so.

1.3 This policy applies to all the processing of personal data we are responsible for including processing by joint controllers, contractors and processors and applies to all formats or media on which the data are stored.

1.4 A glossary of the terms used throughout the policy is included at Appendix 1.

## 2. Objectives

2.1 The objectives of this policy are to ensure that:

- All personal data is processed in keeping with the data protection principles in the GDPR, including being:
  - processed lawfully;
  - fairly and in a transparent manner;
  - processed only for specific, explicit and legitimate purposes;
  - adequate, relevant and accurate;
  - not kept longer than is necessary; and
  - processed securely.
- Data subjects' rights around how their data is handled are upheld and can be exercised by data subjects;

- Data sharing is carried out in a safe and secure manner, and in keeping with the principles and data subjects' rights;
- Data is not transferred outside of the UK or European Union (EU) except in limited circumstances and subject to ExtraCare consent;
- Any data security breaches are reported and managed appropriately; and
- ExtraCare can demonstrate its accountability and compliance with legal requirements.

2.2 Where we process special category and criminal offence data, data protection law requires us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles listed above, and to have policies regarding the retention and erasure of such personal data. This policy, together with other ExtraCare policy and work instructions fulfils this requirement.

2.3 Although data protection is synonymous with cyber security this policy is not about cyber security. Cyber security is about how we protect the devices we use and the services we access to prevent the use of unauthorised access to personal information whereas Data Protection is about our understanding of data subject rights and how personal information is collected, used, stored, and shared.

## 3. Scope of Policy

3.1 This policy applies to all Board Members, staff, volunteers, consultants, Agency staff and others employed by ExtraCare or its subsidiary.

3.2 All those with access to personal data have a crucial role to play to ensure that ExtraCare maintains the trust and confidence of the individuals about whom ExtraCare processes personal data by compliance with ExtraCare's legal obligations and protecting ExtraCare's reputation.

3.3 All members of staff must read, understand, and comply with this policy when processing personal data in the performance of their tasks and must observe and comply with all controls, protocol, practices and training to ensure compliance.

3.4 Negligent or malicious non-compliance with policy or work instructions will be dealt with through the disciplinary process.

## 4. Responsibilities

4.1 All those who have access to personal data in the performance of their role with ExtraCare have a responsibility to comply with Data Protection legislation and regulation. Specific responsibilities are detailed below.

| | |
|---|---|
| Board | Responsible for the overview and scrutiny of the data protection arrangements in place at ExtraCare. |
| Audit and Assurance Committee | Receive reports from the Data Protection Officer in respect of reported data breaches and recommend appropriate remedial action where appropriate. |
| Executive Leadership Team | Ensure compliance with relevant legislation and the ExtraCare's own policies. |
| Senior Management Team | Responsible for ensuring their team read, understand, and comply with this policy before carrying out tasks that involve handling personal data. Ensure that Data Protection Impact Assessments are undertaken where required and address any recommendations/comments on these raised by the DPO. |
| PMO | Responsible for ensuring that Data Protection Impact Assessments are carried out where projects will involve or affect our processing of personal data. |
| Data Protection Officer (DPO) | Responsible for:<br>• Informing and advising on our obligations to comply with the UK GDPR and other data protection laws;<br>• Monitoring compliance with the UK GDPR and our data protection policy;<br>• Advising on and monitoring compliance of internal data protection activities including completion of Information Asset Registers and Records of Processing Activity;<br>• Raising awareness of data protection issues and monitoring staff training;<br>• Advising on and monitoring data protection impact assessments; and |

| | |
|---|---|
| | • Liaison with the ICO and to be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc).<br><br>The DPO can be contacted at:<br>• Privacy@extracare.org.uk; or<br>• Databreach@extracare.org.uk<br>The DPO may seek specialist advice where needed. |
| Chief Information Security Officer (CISO) (Head of IT) | Responsible for:<br>• The proposal, advice on and implementation and maintenance of technical controls to assist in ensuring data privacy in IT systems;<br>• Developing, implementing, and enforcing suitable and relevant information security processing and protocols to comply with data protection regulation;<br>• Ensuring all electronic equipment and assets have adequate security measures to comply with data protection regulation;<br>• Ensuring policies and procedures in place to cover all aspects of information system security; and<br>• Advising on and monitoring relevant systems to assist the DPO to ensure that Asset Registers and Records of Processing Activity are in place and complete for all relevant electronic information systems which process personal data. |
| Governance and Compliance Team | Responsible for:<br>• Supporting the DPO in ensuring ExtraCare compliance with this policy;<br>• Monitoring the data breach inbox; maintaining the Data Breach log, investigating, and responding where appropriate;<br>• Provide templates for use e.g., Data Privacy Impact Assessments and ensure good document management and storage of completed documents; and<br>• Monitoring the privacy inbox, maintaining the Information Rights log, collating relevant information, and responding where appropriate. |
| All Managers | All Managers are responsible for:<br>• Ensuring completion of Information Asset Registers and Records of Processing Activity for relevant processed personal data both electronic and hard copy; |

| | |
|---|---|
| | • Ensuring that a Data Privacy Impact Assessment (DPIA) is completed where there are changes to the processing of personal data; and<br>• Ensuring that data breaches are notified, and appropriate action taken. |
| Training Team | • Provision of a comprehensive eLearning package for all staff which incorporates key areas of data protection including handling requests, data sharing, information security, personal data breaches and records management;<br>• Regular review of Data Protection training to ensure remains accurate and up to date; and<br>• Provision of regular reports to Managers and the Governance and Compliance Team to provide data and information on completion of Data Protection training. |
| All Staff | All colleagues are responsible for:<br>• Reading, understanding, and complying with this policy before carrying out tasks that involve handling personal data regardless of the format of that data;<br>• Completing a Data Privacy Impact Assessment where appropriate;<br>• Completing Information Assets Registers and Registers of Processing Activity where appropriate;<br>• Ensure eLearning is completed and up to date;<br>• Reporting any suspected breaches of this policy to databreach@extracare.org.uk; and<br>• Reporting any requests involving personal data to privacy@extracare.org.uk. |

## 5. Monitoring & Review

5.1 To meet our data protection obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. This includes technical measures, for instance around IT and network security, as well as organisational measures such as policies, operational procedures, and guidance to give appropriate direction on the application of the data protection legislation, and including all relevant policies as set out in section 9 below.

5.2 Compliance with this policy will be monitored by the DPO with support from the Governance Team and supported by periodic reviews undertaken by internal audit.

5.3 The success of this policy will be measured through compliance with the risk appetite approved by the Board and through the ongoing review of breach reporting and data subject rights requests.

5.4 Data Protection, breach and SAR reporting are reviewed by the Audit and Assurance Committee at each of their meetings and bi-monthly by ELT.

5.5 ExtraCare will carry out a fundamental review of this policy every three years and, as a Corporate Policy, will be approved by the Board. A review may be carried out sooner than three years if legal regulatory or internal changes occur impacting on the substance of the policy. An earlier review may also be undertaken in response to learnings from any incidents/feedback from users.

## 6. Risk Management

6.1 The Board of Trustees have identified a breach of legislative and regulatory requirement as a corporate risk for which they have a minimalist appetite. Risks arise from processing personal data and a breach of data protection law represents and financial and reputational risk for ExtraCare.

6.2 Compliance with this policy, other related policies, associated work instructions and other related documentation, controls and reduces the risk and ensures that the Trust meets its regulatory and compliance obligations.

## 7. Statement of Commitment

7.1 ExtraCare is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about residents, customers, staff, or those who work or interact with us.

7.2 We publish our Privacy notice on the ExtraCare website, and additional or updated notices are provided where appropriate.

7.3 We provide mandatory Data Protection training for all staff within one month of start date and refresher training at least bi-annually thereafter. Additional role-related training is provided where appropriate. Further information is provided in policies and other documents linked to this policy and extra guidance may be issued through other communication channels as and when required.

7.4 We review all personal data breaches and near misses and these must be communicated through databreach@extracare.org.uk. We assess whether breaches need to be reported to the Information Commissioners Office (ICO). We commit to taking appropriate action and notifying data subjects where appropriate.

7.5 We commit to undertaking Data Protection Impact Assessments where the processing of personal data is deemed to be high risk and to ensure that compliance and 'privacy by design' is integral to any service we offer.

7.6 We commit to recording our processing activities and will identify special category or high risk data to ensure compliance with legislation.

## 8. Additional arrangements

### 8.1 Terminology

**Personal data** is any information relating to a natural living person who is either identified or identifiable. This includes but is not limited to our Trustees, residents, staff, customers, and others who we may come into contact with in carrying out our role at ExtraCare.

'**Special categories'** of personal data includes information about a person's: race or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health; genetic and biometric data; sexual life or sexual orientation.

**Other personal data** such as bank details may be considered 'sensitive' but will not be subject to the same legal restrictions as the data listed in the special categories above.

**Processing** means anything that can be done to personal data, including but not limited to, collecting, storing, using, sharing, and disposing of data.

**A Data subject** is the person to whom the personal data relates.

**A controller** determines the reasons for which personal data is collected, and the ways that it will be processed.

**A processor** is an organisation which is responsible for processing personal data on behalf of a controller. For example, a supplier of web-hosted software that the controller uses to hold personal data in, or a repairs contractor who needs to receive customer names and addresses to be able to carry out the repairs.

**Information about criminal proceedings or offences** is regarded as a separate type of personal data and is subject to strict legal restrictions.

**The Information Commissioner's Office**, or ICO, is the UK's data protection regulator. The ICO produces guidance on how to implement good data protection practices and can take action when a breach of data protection law occurs.

## 8.2 Data Protection by Design and Default

8.2.1 When planning projects/ new ways of working that involve or affect our processing of personal data, we will consider the data protection implications, and how we ensure we meet legal and good practice requirement, from the planning stages.

8.2.2 One way that we will do this is by using **Data Protection Impact Assessments** (DPIAs). A DPIA is a process which helps to minimise the data protection risks involved in projects, processes and activities involving the processing of personal data.

8.2.3 We will complete a DPIA for any project involving the use of personal data, including new systems and revisions or updates to systems.

8.2.4 ExtraCare's Data Privacy Impact Assessment Work Instruction provide full details and a template for conducting a DPIA. The DPO's advice must be sought when carrying out DPIAs.

## 8.3 Data Protection Principles

8.3.1 The UK GDPR is based on a core set of principles that we must observe and comply with at all times.

8.3.2 **Principle 1 - Fair, Lawful and Transparent Processing**
In order to collect and process data for any specific purpose ExtraCare must always have a **lawful basis** for doing so:

a) Consent of the data subject (this must be informed and explicit consent);
b) Necessary for a contract with the data subject;
c) Necessary for us to comply with a legal obligation;
d) Necessary to protect someone's 'vital interests' ('life or death');
e) Necessary for the performance of a task in the public interest, and the task has a clear basis in law; and/or
f) Necessary for us to pursue our legitimate interests, or the legitimate interests of another organisation, unless the interests are overridden by the interests, rights, and freedoms of the data subject.

We generally rely on b), c), d), e) and f) as our lawful bases for processing data. Where we process data on the basis of f) 'legitimate interest' we will be able to explain what our interest is and how we have assessed and ensured compliance with the interests of the data subject.

8.3.3 We do not normally rely on consent as our general basis of processing personal data but where we do, we will ensure requests for consent are:

- Clear and specific;
- Not bundled together;
- Use opt-in rather than opt-out methods;
- Name any third parties who rely on the consent;
- Ensure data subjects can easily withdraw their consent;
- Comply with the Privacy and Electronic Communications Regulations (PECR) which requires that we obtain consent before sending unsolicited electronic direct marketing messages; and
- Commit to adhering to the Telephone Preference Service (TPS) which requires that we do not cold call anyone who is registered with the TPS.

8.3.4 We will identify the lawful basis for processing and document this for each specific purpose, or group of related purposes on our **Records of Processing Activity**.

8.3.5 To be lawful, fair and transparent, our data processing is explained in our Privacy Policy which contains our full Privacy Notice and is published on our website www.extracare.org.uk.

Our Privacy Notice Includes:

- Our identity and contact details and those of our DPO,
- The reasons and legal basis for processing personal data;
- An explanation of the legitimate interests pursued;
- The consequences to data subjects of not providing data needed for contractual or statutory reasons;
- Any automated decision making or profiling;
- Who we share the data with;
- If we send any data outside of the UK and the EU and the safeguards in place if we do;
- How long the data is stored; and
- The legal rights individuals have around their data including the right to withdraw consent and to complain to the ICO.

8.3.6 We will make available additional Privacy notices where appropriate, e.g., CCTV.

8.3.7 Where possible and appropriate relevant Privacy Notices should be communicated with data subjects at the time of collecting their data, or within one month of receiving their data from a third party. Our full Privacy Notice is available at www.extracare.org.uk.

8.3.8 **Principle 2 - Purpose Limitation**

We will only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to the data subject before the personal data is collected.

8.3.9 We must ensure that we do not process any personal data, obtained for one or more specific purposes, for a new purpose that is not compatible with the original purpose. If we intend to do this, we must inform the data subjects before using their personal data for the new purpose and, where the lawful basis relies on consent, we must obtain such consent again.

8.3.10 **Principle 3 – Data Minimisation**

The data that we collect, and process must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed. We will not access data that we have no reason to access, nor will we share or allow access to data with those who have no reason to see that data. We do this through role-based access controls and using systems and standardised processes which help to ensure that only relevant information is captured.

8.3.11 **Principle 4 – Accuracy**

We endeavour to ensure that the data we collect, and hold is accurate, complete, and where appropriate kept up to date.

8.3.12 We endeavour to implement maintenance processes to avoid unnecessary duplication and reduce the risk of errors in recording and reporting. This will include periodic data review and testing processes where personal data is held.

8.3.13 All staff must make any changes to their personal data on ITrent within one month of the change occurring. Staff are asked to review and update their personal data on ITrent at least biannually.

8.3.14 We will correct any personal data that we find to be inaccurate. Where appropriate, any inaccurate or out of date records should be deleted or destroyed. We may retain records of inaccurate or out of date information where it is necessary for clinical and corporate governance purposes to provide a full audit trail.

8.3.15 **Principle 5 – Storage Limitation (Data Retention)**

The personal data that we collect and process, must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements).

8.3.16 Storing data for longer than is necessary may increase the severity of a data breach and may also lead to increased costs associated with storage. Data should not be kept 'just in case'. A Retention Schedule is contained in the Records Management Policy which takes account of legal and contractual requirements and limitation periods, and good industry practice. We may need to keep data for longer than standard retention periods where it is needed for litigation, to respond to complaints, or for other governance processes.

8.3.17 **Principle 6 – Security, Integrity and Confidentiality**
The personal data that ExtraCare collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction, or damage, and against unauthorised or unlawful processing.

8.3.18 We use both technical and organisational security measures to protect the integrity of personal data including protecting data from unauthorised or unlawful processing, or from accidental loss, destruction, or damage.

8.3.19 Security measures must be appropriate to the level of risk involved in the data and the processing. Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures. Our electronic systems and physical storage have appropriate access controls applied.

8.3.20 Personal data must not be sent to or from colleagues' personal accounts – email, Facebook Messenger, WhatsApp, etc or stored in personal or unapproved (by IT) systems and tools (for example Dropbox, WeTransfer, Zoom)

8.3.21 Further detail on security is contained in the Information Security Policy.

8.3.22 **Principle 7 – Accountability**
To demonstrate and support our compliance with data protection legislation we:

- Have appointed a DPO;
- Have appropriate policies and procedures in place;
- Train all our colleagues in Data Protection;
- Keep records of the processing activities we carry out;
- Undertake DPIAs where appropriate;
- Carry out regular reviews of our activities;
- Report and investigate data security breaches; and
- Undertake due diligence on our suppliers and partners and put in place appropriate arrangements when we share information with them or they process it on our behalf, including as set out in section 8.5 below.

8.3.23 Records of processing activity include information about how and why we are processing personal data, what data we hold, and the legal basis for the processing, as well as any third parties the data is shared with, including any transfers outside of the EU, and the safeguards in place if data is transferred outside the EU.

### 8.4 Data Subject Rights

8.4.1 The GDPR provides data subjects with a number of rights in relation to their personal data:

- **Right to withdraw consent** – where the lawful basis relied upon is consent, the right to withdraw such consent at any time without having to ask why;
- **Right to be informed** – the right to be provided with certain information about how we collect and process the data subject's personal data;
- **Right of subject access** – the right to receive a copy of the personal data that we hold including certain information about how ExtraCare have processed the data subject's personal data;
- **Right to rectification** – the right to have inaccurate personal data corrected or incomplete data completed;
- **Right to erasure (right to be forgotten)** – the right to ask for their personal data to be deleted or destroyed;
- **Right to restrict processing** – the right to ask ExtraCare to restrict processing in certain circumstances depending on whether ExtraCare's legitimate interest grounds for processing override those of the data subject.
- **Right to data portability** – in limited circumstances, the right to ask ExtraCare to transfer a copy of their data to a third party in a structured, commonly used machine readable format;
- **Right to object to direct marketing** – the right to request that we do not process the data subject's personal data for direct marketing purposes;
- **Right to object to decisions based solely on automated processing including profiling** – the right to request that they are not subject to automated decision making or profiling that has legal or other significant effects on the data subject and the right to request human intervention; and
- **Right to be notified of a personal data breach** – the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms.

8.4.2 ExtraCare will respond to and fulfil all valid requests as soon as possible and comply with the legal deadlines (these are generally one month but can be extended in certain situations). **A supporting work instruction on Subject Access Requests exists.**

## 8.5 Data Processors

8.5.1 Contractors who process data as part of the work they are doing on behalf of ExtraCare are 'data processors'. When working with data processors we will carry out appropriate due diligence checks to ensure that they can provide sufficient guarantees that they will comply with data protection legislation, including keeping data secure and cooperating with us to ensure we uphold data subject's rights.

8.5.2 We will appoint data processors on the basis of a legally binding, written contract, that requires them to, amongst other things:

- Only process personal data based on our instructions;
- keep the data secure;
- assist us to comply with our legal obligations and uphold data subjects' rights;
- delete or return the data at the end of the contract; and
- allow inspections and audits of their processing activities.

8.5.3 We will only share personal data with third parties when the sharing has one or more appropriate legal bases and is carried out in in accordance with data protection legislation.

## 8.6 Data Security Breaches

8.6.1 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.

8.6.2 A data breach "near miss" is where a breach has occurred, but the breach is unlikely to result in a risk to individuals.

8.6.3 As soon as a data breach or near miss is identified it should be reported to the Data Protection Office by emailing databreach@extracare.org.uk.

8.6.4 All data breaches and near misses will be investigated appropriately and corrective and preventative action taken where necessary.

8.6.5 Any personal data breaches of a significant nature which are likely to result in a risk to data subjects and are reportable to the ICO, will be reported to the ICO within 72 hours of becoming aware of the breach.

8.6.6 Where a data breach causes a high risk to data subjects, we will also inform the data subjects, without undue delay, to allow them to take any action that may help protect them and their data. **A supporting work instruction on Data/Information Security Breaches exists.**

## 8.7 Sharing Information outside of Data Protection Regulation

8.7.1 **Mental Capacity**

The nature of ExtraCare's residents means that we may provide services to individuals who may not be able to make decisions for themselves due to mental capacity and where we may be required to share information in an individual's best interests. Where an individual is unable to make decisions for themselves, we will share relevant information with those with an interest in their welfare, including those who have deputyship or lasting powers of attorney for the individual concerned.

8.7.2 **Deceased Individuals**

Data Protection regulation and legislation only applies to living individuals. However, the nature of our work means that we have an ethical duty to respect confidentiality after the death of an individual. Where medical records are requested beyond death, we will respond to the request in accordance with the principles of the Access to Health Records Act 1990.

8.7.3 For requests other than medical information we will balance the interests of preserving confidentiality and what is known about the deceased's individual's wishes with the reasons for wanting access to the information in question, and the status of the individual who is asking for the information.

## 9. Other Relevant ECCT Policies & Documents

| | |
|---|---|
| **General** | • Information Security Policy<br>• Records Management Policy<br>• Information Classification Policy<br>• Privacy Policy;<br>• Complaints Management Policy;<br>• CCTV Policy;<br>• Safeguarding Policy;<br>• Whistleblowing Policy;<br>• Social Media Policy;<br>• Recruitment Policy;<br>• Dignity, Privacy and Respect Policy;<br>• Training and Development Policy;<br>• IT Security Policy<br>• Disciplinary Policy<br>• Grievance Policy<br>• Staff Handbook<br>• Major Incidents & Escalation Policy<br>• Incident Reporting Policy<br>• Trustee Escalation Statement |
| **Work Instructions** | • Data Protection Breach Work Instructions<br>• Subject Access Request Work Instructions<br>• Privacy Impact Assessment Work Instructions |
| **Other** | • Staff Handbook<br>• Employment contract<br>• Job Descriptions<br>• Data Protection e-learning – revised 2022<br>• Cyber Security e-learning |

## 10. Relevant Legislative & Regulatory Requirements

| Legislation | Regulation | Guidance |
|---|---|---|
| Data Protection Act 2018 | UK General Data Protection Regulation | ICO Codes of Practice:<br>• Data Sharing;<br>• CCTV<br>• Employment Practices<br>• Direct Marketing |
| Computer Misuse Act 1990 | Privacy and Electronic Communications (EC Directive) Regulations 2003 | |
| Mental Capacity Act 2005 | | |
| Care Act 2014 | | |
| Human Rights Act 1998 | | |
| Equality Act 2010 | | |