Abbeyfield (East Devon) Society Ltd

Abbeyfield (East Devon) Society Limited is a Member of The Abbeyfield Society.
Housing Corporation No.H2776. Company No: 15141319 Registered Charity No: 1206411

TITLE	**Data Protection Policy**			
Policy ref:	LG013P		Approval date	October 2024
Owner	Director of Legal and Compliance		Planned review date	October 2027
Approved by	Trustee..... October 2024			

1 Background	This Data Protection Policy sets out how Abbeyfield East Devon Society (AED) handles the Personal Data of its residents (and their families), suppliers, employees, workers and other third parties. This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, residents, supplier contacts, website users or any other Data Subject.
2 Objectives	Through the delivery of this policy, we aim to: • Ensure that records required to be kept for legal and other relevant purposes are kept for the appropriate period; • Manage and maintain records in such a way that there is full compliance with all regulatory and statutory requirements, and in particular, to avoid enforcement action from the Information Commissioner's Office. • Ensure records are stored in the most economical way, are accessible and are disposed of in a way which is auditable and meets all legal, environmental and other requirements. • Ensure records are kept secure and safe from loss, damage or tampering and are destroyed in a secure manner. • Protect our reputation.
3 Scope	This policy applies to all Abbeyfield East Devon Society (AED) employees, workers, contractors, agency workers, directors, volunteers and others. This policy sets out what we expect from all staff in order for AED to comply with applicable law. Compliance with this policy is mandatory and any breach of it may result in disciplinary action.

4 Policy **4.1**	**POLICY STATEMENT** We will ensure the correct and lawful treatment of Personal Data and full compliance with GDPR to protect the privacy of our residents and staff and to maintain confidence in the organisation. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that everyone is expected to take seriously at all times. Abbeyfield is exposed to potential fines of up to approximately £17 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR. All staff who have regular contact with residents, suppliers, or deal in any other manner with the Personal Data that Abbeyfield East Devon has access to, are responsible for complying with this policy and need to implement appropriate practices, processes, controls and undergo training to ensure compliance. **DATA PROTECTION OFFICER (DPO)** The DPO is responsible for overseeing this policy and, as applicable, developing related policies and privacy guidelines. Any questions about the operation of this policy, the GDPR, or any concerns that this policy is not being followed, should be brought to the attention of the DPO. In particular, the DPO should be contacted in the following circumstances: • Where there is uncertainty about the lawful basis being relied upon to process Personal Data (including the legitimate interests used by AED) (see Section 4.3); • When relying upon Consent and/or need to capture Explicit Consent (see Section 4.3.2); • Before drafting Privacy Notices or Fair Processing Notices (see Section 4.3.3); • Where there is uncertainty about the retention period for the Personal Data being Processed (see Section 4.7); • Where clarification is needed about what security or other measures are needed to protect Personal Data; • If there has been a Personal Data Breach (Section 4.8.2); • Where there is uncertainty about the basis for transferring Personal Data outside the EEA (see Section 4.9); • If assistance is needed to deal with any rights invoked by a Data Subject (see Section 4.10**Error! Reference source not found.**); • When engaging in a significant new, or change in, Processing activity which is likely to require a Data Protection Impact Assessment (DPIA) (see

Section 4.13) or when there is an intention to use Personal Data for purposes other than what it was collected for;

- Where help is needed to ensure compliance with applicable law when carrying out direct marketing activities; or
- Where help is needed with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see Section 4.13).

PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (See 4.5 Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (See 4.6 Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (See 4.7 Data Minimisation).

(d) Accurate and where necessary kept up to date (See 4.8 Accuracy).

(e) 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 (See 4.9 Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (See 4.10 Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (See 4.11 Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (See 4.12 Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

Lawfulness and Fairness

	Abbeyfield may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.
4.2	The GDPR allows Processing for specific purposes, some of which are set out below: **(a)** the Data Subject has given his or her Consent; **(b)** the Processing is necessary for the performance of a contract with the Data Subject; **(c)** to meet our legal compliance obligations; **(d)** to protect the Data Subject's vital interests; **(e)** to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in our Privacy Notice. We must identify and document the legal ground being relied on for each Processing activity.
4.3	**Consent** A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if there is an intention to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented. Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Category Personal Data. Usually we will

4.4	be relying on another legal basis (and will not require Explicit Consent) to Process most types of Special Category Data. Abbeyfield East Devon obtains Explicit Consent in the forms that residents (or the person with legal responsibility for them) sign upon admission. **Transparency (notifying data subjects)** The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices, which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. Whenever we collect Personal Data directly from residents, we must give them or refer them to the Privacy Statement, which explains what Personal Data we are collecting and why we need it. When Personal Data is collected indirectly (for example, from a doctor, social worker or other source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving it. **PURPOSE LIMITATION** Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purpose and basis on which data is to be collected and processed should be determined before the processing commences. **DATA MINIMISATION** Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. AED may only Process Personal Data when the performance of its duties requires it. We cannot Process Abbeyfield's Personal Data for any reason unrelated to its business. AED may only collect Personal Data that it requires for its duties and must not collect excessive data. Any Personal Data collected must be adequate and relevant for the intended purposes it has been collected for.

4.5	We must ensure that when Personal Data is no longer needed, it is deleted or anonymised in accordance with our data retention guidelines.
4.5.1	**ACCURACY** Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. We will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data. **STORAGE LIMITATION** Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. Abbeyfield East Devon must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected including for the purpose of satisfying any legal, reporting or safeguarding requirements. Our Records Management Policy (LG015P) includes a Records Retention Schedule to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.
4.5.2	**SECURITY INTEGRITY AND CONFIDENTIALITY** **Protecting Personal Data** Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and passwords where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. We are responsible for protecting the Personal Data we hold. We

	must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of or damage to the same. We must exercise particular care in protecting Special Category Personal Data from loss and unauthorised access, use or disclosure. All staff must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. These include the use of passwords, security of doors, IT systems, laptops, mobile devices, filing cabinets etc. We must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows: **(a)** Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it. **(b)** Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
4.5.3	**(c)** Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes. **Reporting a Personal Data Breach** The GDPR requires Data Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject. Any actual or potential Personal Data Breach must be reported immediately to the DPO who will notify Data Subjects or any applicable regulator where we are
4.6	legally required to do so. All evidence relating to the actual or potential Personal Data Breach should be preserved. **TRANSFER LIMITATION** The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals is not undermined. Personal Data originating in one country is transferred when it is transmitted, sent, viewed or accessed across borders in or to a different country.
4.7	If this may be occurring, the DPO should be contacted for advice and instructions. **DATA SUBJECT'S RIGHTS AND REQUESTS** **Data Subject's Rights** Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

4.8	**(a)** withdraw Consent to Processing at any time; **(b)** receive certain information about the Data Controller's Processing activities; **(c)** request access to the Personal Data that we hold about them; **(d)** ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data; **(e)** restrict Processing in specific circumstances; **(f)** challenge Processing which has been justified on the basis of our legitimate interests or in the public interest; **(g)** prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else; **(h)** be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; **(i)** make a complaint to the Information Commissioner's Office; and **(j)** in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.
4.9	We must verify the identity of an individual requesting data under any of the rights listed above (and not allow third parties to persuade us into disclosing Personal Data without proper authorisation). Data Subject requests must be immediately forwarded to the DPO.
4.10 **4.10.1**	**National Data Opt-Out (care resident data)** The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes. AED does not use or share residents' personal data for research and planning. Abbeyfield East Devon reviews all of its data processing on an annual basis to assess if the national data opt-out applies. This is recorded by the DPO in our Record of Processing Activities. All new processing is assessed to see if the national data opt-out applies. If any data processing falls within scope of the national data opt-out we use Message Exchange for Social Care and Health (MESH) to check if any of our residents have opted out of their personal health data being used for research and planning.
	Sharing Personal Data

	Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. We may only share the Personal Data we hold with third parties, such as our service providers if: **(a)** they have a need to know the information for the purposes of providing the contracted services; **(b)** sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained; **(c)** the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; **(d)** the transfer complies with any applicable cross border transfer restrictions; and **(e)** a fully executed written contract that contains GDPR approved third party clauses has been obtained.
4.10.2	Where in doubt, the matter should be referred to the DPO. **Record Keeping** The GDPR requires us to keep full and accurate records of all our data Processing activities. These records should include at a minimum: **(a)** our name and contact details. **(b)** a clear description of the Personal Data types, Data Subject types, Processing activities, Processing purposes and third-party recipients of the Personal Data we hold. **(c)** Personal Data storage locations. **(d)** Personal Data transfers. **(e)** the relevant retention period and **(f)** a description of the security measures in place.
4.11	In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows. **DATA SECURITY AND PROTECTION TOOLKIT (DSPT)** The DSPT is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

4.12	All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. The DSPT self-assessment tool will be completed centrally and published annually on behalf of Abbeyfield's registered care services. **PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)** We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles. We must assess what Privacy by Design measures can be implemented on all programs and systems that Process Personal Data by taking into account the following: **(a)** the state of the art. **(b)** the cost of implementation. **(c)** the nature, scope, context and purposes of Processing; and **(d)** the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing. Whenever we are considering the use of new systems, software or processes which may impact on Abbeyfield's processing of Personal Data, the DPO should be consulted, and we must ensure the data protection implications have been appropriately thought through and documented via a DPIA. **AUDITS** Managers will conduct Data Security audits at least annually and are responsible for taking timely action to remedy any aspects of non-compliance.
4.13	**TRAINING** All staff are required to undergo data protection training to enable them to comply with data privacy laws. Managers with responsibility for data security and protection will receive training suitable for their role. **DEFINITIONS** **Consent:** agreement which must be freely given, specific, informed and be an

unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. Abbeyfield is the Data Controller of all Personal Data relating to our staff and Personal Data used in our business for our own commercial purposes.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the data protection manager, who has responsibility for data protection compliance across all of the organisation's operations. Our DPO is the Director of Legal and Compliance.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data. Each of our residents will be Data Subjects.

EEA: the European Economic Area, including all 28 countries in the EU, together with Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

GDPR: the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Information Commissioner: is the UK's independent regulator for Data Protection and Freedom of Information, with key responsibilities under the Data Protection Act 2018 (DPA) and Freedom of Information Act 2000 (FOIA), as well as a range of other related legislation. As set out in the DPA, the Information Commissioner is a Corporation Sole (a single legal entity).

National Data Opt-Out: a service that allows patients/service users to opt out of their confidential health and care information being used for research and planning. All organisations providing or coordinating publicly funded health or care in England will need to comply with the opt-out. This includes private, voluntary and independent organisations and adult social care.

Personal Data: any information that allows us to identify a data Subject from that data alone or in combination with other identifiers we possess or could reasonably access. Personal Data includes Special Category Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: anything that compromises the security, confidentiality, integrity or availability of Personal Data or the safeguards that we put in place to protect it. The loss, or unauthorised access, disclosure or acquisition of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: notices or policies setting out information that may be provided to Data Subjects when the organisation collects information about them e.g. employee privacy notices or the website privacy policy.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Special Category Personal Data: information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health related information, sexual life, sexual orientation, biometric or genetic data. Although Personal Data relating to finances and criminal offences and convictions is not classed as Special Category, it is nonetheless sensitive. As a care provider, we will have access to a great deal of Special Category and sensitive Personal Data about residents receiving care, e.g. their medical history.

5 Finance, Value for Money & Social Value	The consequences of failing to comply with data protection law can be far reaching in terms of potential fines, harms to individuals as a result of misuse of their personal data and reputational damage.
6 Linked policies	Access to Personal Records (LG039P) Confidentiality (R005P) Information Security (LG023P) Records Management (LG015P)
7 Relevant Legislation / Regulation	General Data Protection Regulations (GDPR) Data Protection Act 2018
8 Guidance	Data Security and Protection Toolkit (DSPT) The UK Caldicott Guardian Council Understanding the national data opt out Information Commissioner's Office (ICO)
9 Review	Every 3 years, subject to any regulatory or legislative updates.
10 Procedure(s)	None.