Berhamsted and Hemel Hempstead Society Data protection policy

1. Interpretation
    - **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. We are the Data Controller of all Personal Data relating to our Personnel 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 Manager (DPM)":	the data protection manager, who has responsibility for data protection compliance across all of the Society's operations. Our DPM is Christine Hopcraft.
"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).

“General Data Protection Regulation (GDPR)”:	the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.
“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.
“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 Sensitive 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.
“Personnel”:	all employees, trustees, volunteers, contractors, agency workers and others.
“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 we collect 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.
“Sensitive Personal Data”:	information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions. In the course of our activities, we will have access to a great deal of Sensitive Personal Data about our residents e.g. their medical history.

“Society”:	The Abbeyfield (Berkhamsted and Hemel Hempstead) Society Limited

2. Introduction

This Data Protection Policy (“Policy”) sets out how the Society (”we”, “our”, “us”, “the Society”) handles the Personal Data of our 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.

This Policy applies to all Personnel (”you”, “your”). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for the Society to comply with applicable law. Your compliance with this Policy is mandatory. Any breach of it may result in disciplinary action.

3. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will preserve the dignity and privacy of our residents. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Society 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 Personnel who have regular contact with residents, suppliers or deal in any other manner with the Personal Data that the Society has access to, are responsible for complying with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPM is responsible for overseeing this Policy and, as applicable, developing Related Policies and Privacy Guidelines. Please contact them with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being followed. In particular, you must always contact the DPM in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Society) (see *Section 1* below);
- if you need to rely on Consent and/or need to capture Explicit Consent (see *Section 2* below);
- if you need to draft Privacy Notices or Fair Processing Notices (see *Section 3* below);
- if you are unsure about the retention period for the Personal Data being Processed (see *Section* 8 below);
- if you are unsure about what security or other measures you need to implement to protect Personal Data;
- if there has been a Personal Data Breach (*Section 2* below);
- if you are unsure on what basis to transfer Personal Data outside the EEA (see *Section 10* below);
- if you need any assistance dealing with any rights invoked by a Data Subject (see *Section 11*);
- whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see *Section 4* below) or plan to use Personal Data for purposes other than what it was collected for;
- If you need help complying with applicable law when carrying out direct marketing activities; or
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see *Section 5* below).

4. 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:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
- Collected only for specified, explicit and legitimate 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 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 (Security, Integrity and Confidentiality).

- Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (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).

5. Lawfulness, Fairness, Transparency
    - **Lawfulness and Fairness**

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

You 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.

The GDPR allows Ppocessing for specific purposes, some of which are set out below:

- the Data Subject has given his or her Consent;
- the processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests;
- 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.

You must identify and document the legal ground being relied on for each Processing activity.

- **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 you intend 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 sensitive personal data. Usually we will be relying on another legal basis (and will not require Explicit Consent) to process most types of Sensitive Data.

The Society obtains Explicit Consent by using the forms residents (or the person with legal responsibility for them) sign upon admission. These consent forms are to be given to the Senior House Manager and stored in their file after being scanned and uploaded to the cloud.

- **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), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving it.

6. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only Process Personal Data when the performance of your duties requires it. You cannot Process the Society’s Personal Data for any reason unrelated to your work.

You may only collect Personal Data that you require for your duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes it has been collected for.

You must ensure that when Personal Data is no longer needed, it is deleted or anonymised in accordance with our data retention guidelines.

7. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You 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. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

8. 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.

You 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 we originally collected it including for the purpose of satisfying any legal, reporting or safeguarding requirements.

We will maintain retention policies and procedures 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.

9. 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. You are responsible for protecting the Personal Data we hold. You 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. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You 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 ensuring that offices are kept locked at all times when unoccupied, all computers are password protected and not left on when not in use, all paperwork which may be subject to Data Protection is kept confidential and secure at all times and any other instructions that you may be given verbally or in writing at any time.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- 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.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so

If you know or suspect that a Personal Data Breach has occurred, immediately contact the DPM using the details set out below. In the first instance a phone call should be made to the DPM to report the breach, a written report giving full details should be made and sent to the DPM (if emailed it MUST be password protected). If you are unable to reach the DPM then you should contact the Business Manager or the Executive Chair. You should preserve all evidence relating to the potential Personal Data Breach.

10. 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. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

If you think that this may be occurring, please contact the DPM for further instructions.

11. Data Subject's rights and requests

- **Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:**

- withdraw Consent to processing at any time;
- receive certain information about the Data Controller's processing activities;
- request access to the Personal Data that we hold about them;
- 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;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the Information Commissioner's Office; and
- 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.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the DPM.

12. Accountability

- **The Society must have adequate resources and controls in place to ensure and to document GDPR compliance including:**

- Implementing Privacy by Design when processing Personal Data and completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this Privacy Standard and relevant Privacy Notices;
- regularly training Personnel on the GDPR, this Privacy Standard and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Society must maintain a record of training attendance by Personnel; and

- regularly testing the Privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

- **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:

- our name and contact details;
- 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;
- Personal Data storage locations;
- Personal Data transfers;
- the relevant retention period and
- a description of the security measures in place.
  In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

- **Training**

We are required to ensure all Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance. You must undergo all mandatory data privacy related training.

- **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.

You must assess what Privacy by Design measures can be implemented on all programmes and systems that Process Personal Data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

Whenever you are considering the use of new systems, software or processes which may impact on the Care Provider’s processing of Personal Data, you

should consult the DPM, and make sure that the data protection implications have been appropriately thought through and documented.

- **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.

You may only share the Personal Data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- 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;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains GDPR approved third party clauses has been obtained.

Where in doubt, discuss the disclosure with the DPM.

13. Changes to this Privacy Standard

13.1 We reserve the right to change this Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Policy.