# DATA PROTECTION PRIVACY NOTICE

The General Data Protection Regulations (the GDPR) will come into force from 25 May 2018. These Regulations contain new requirements concerning how we collect, process, store and erase all personal data (information which can be used to identify a living person) within Avens Care Homes Ltd.

When we collect a person's personal data we will need to tell that person certain things about how we intend to use and process their data and in some cases we may need their consent before we process their data.

## Your Rights and Requests Concerning Your Personal Data

We will process and manage all your Personal Data in line with your rights; in particular your rights to:

- request access to any data we hold about you;
- prevent the processing of your Personal Data for direct-marketing purposes, if so instructed;
- ask to have inaccurate Personal Data amended;
- be forgotten, and have all relevant Personal Data erased (subject to our overriding legal obligations);
- prevent processing which is likely to cause damage or distress to you or anyone else;
- request certain restrictions on the processing of your Personal Data;
- receive a copy of your Personal Data and/or request a transfer of your Personal Data to another Data Controller;
- not be subject to automated decision making;
- be notified of a data security breach which affects your rights and freedoms, without undue delay;
- if you have provided your express consent that your Personal Data may be processed for marketing and advertising purposes, you are entitled to withdraw that consent. Such a withdrawal will not affect any processing of the data completed before consent was withdrawn; and
- to make certain requests to us concerning how your Personal Data is managed.

# Notice Statement

In accordance with the GDPR anyone processing Personal Data must comply with the six principles of good practice. These provide that Personal Data must:

1. be processed fairly, lawfully and transparently;
2. only be used for the purpose for which it was collected;
3. be adequate, relevant and not excessive for the purpose for which it is being processed;
4. be accurate and kept up-to-date;
5. not be kept longer than necessary to fulfil the purpose of its collection; and
6. be kept secure and protected from unauthorised processing, loss, damage or destruction [which includes the data not being transferred to a country or territory outside the European Economic Area unless the Personal Data is adequately protected and/or consent of the Data Subject has been provided].

**1. Fair, Lawful and Transparent Processing**

For Personal Data to be processed lawfully, the basis for the processing must be one of the legal grounds set out in the Enactments. These include, among other things, your written consent to the processing, or that the processing is necessary for the performance of our bookkeeping contract with you.

In the event we collect Personal Data directly from you, this Notice should assist in informing you about:

**1.1** The purpose or purposes for which we intend to process your Personal Data.

**1.2** The types of third parties, if any, with which we may share or disclose your Personal Data.

**1.3** The means with which you can limit our processing and disclosure of your Personal Data.

If we receive Personal Data about you from other sources, we will provide you with this information as soon as possible thereafter.

When sensitive personal data is being processed, additional conditions and securities must be in place to ensure protection.

**2. Processing for Limited Purposes**

In the course of our business, we shall process the Personal Data we receive directly from you (for example, by you completing forms, sending us papers or from you corresponding with us by mail, phone, email or otherwise) and your Personal Data which we receive from any other source.
We shall only process your Personal Data to fulfil and/or enable us to satisfy the terms of our obligations and responsibilities in our role as your Employer or for any other specific purposes permitted by the Enactments. Should we deem it necessary to process your Personal Data for purposes outside and/or beyond the reasons for which it was originally collected, we will contact you first, to inform you of those purposes and our intent and may also apply for your consent.

**3. Adequate, Relevant Non-Excessive Processing**

We will only collect and process your Personal Data as required to fulfil the specific purpose/s of our contract and agreements with you.

**4. Accurate and up to date data**

We shall ensure that all Personal Data held is accurate and up to date and will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. If you become aware that any of your Personal Data is inaccurate, you are entitled to contact us and request that your Personal Data is amended. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

**5. The Timely Processing of the Data**

We will not keep Personal Data longer than is necessary for the purpose or purposes for which it was collected. Once Personal Data is no longer required, we will take all reasonable steps to destroy and erase it.

**6. Keeping Your Personal Data Secure**

Our employees and contracted personnel are bound to our privacy policies, procedures and technologies which maintain the security of all your Personal Data from the point of collection to the point of destruction.

We maintain data security by protecting the confidentiality, integrity and availability of your Personal Data, and when we do so we abide by the following definitions:

**6.1** **Confidentiality:** We ensure that the only people authorised to use your personal data can access it. [Employees are prohibited from accessing and viewing your personal data unless it is necessary to do so]

**6.2** **Integrity:** We will make certain that your Personal Data is accurate and suitable for the purpose for which it is processed.

**6.3** **Availability:** We have established procedures which mean only our authorised Data Users should be able to access your Personal Data if they need it for authorised purposes.
We also maintain security procedures which include, but are not limited to:

**6.4** Secure lockable desks and cupboards. Desks and cupboards shall be kept locked if they hold your personal data.

**6.5** Methods of disposal. Paper documents containing Personal Data are shredded and digital storage devices shall be physically destroyed when they are no longer required.

**6.6** Data Users shall be appropriately trained and supervised in accordance with this Notice which include requirements that computer monitors do not show confidential information to passers-by and that Data Users log off from or lock their PC/electronic device when it is left unattended.

**6.7** Our computers have appropriate password security, boundary firewalls and effective anti-malware defences. We routinely back-up electronic information to assist in restoring information in the event of disaster and our software is kept up-to-date with the latest security patches.

**6.8** One or all of the following measures shall be applied to the personal data held; separating the personal data and/or pseudonymisation and/or the encoding of the data

**6.9** Our Privacy Manager will ensure that this Notice is kept updated in response to any amendments to the Law.

We shall take appropriate security measures against unlawful and/or unauthorised processing of personal data, and against the accidental loss of, or damage to, your Personal Data.
We do not share data outside of the United Kingdom.

Exemptions exist where personal data is not covered by the Data Protection Act. These are known as **complete** and **partial** exemptions and mean that data controllers do not need to adhere to the full rules and regulations of the Data Protection Act.

There are two types of complete exemption:

- Any personal data that is held for a **national security reason** is exempt. This would include monitoring and keeping personal data relating to terror suspects and/or other personal information which puts the UK and its citizens at risk of harm or subject to a security risk.
- Personal data held for domestic purposes only at home (ie a list of friends' names, birthdays and addresses).

## How We Will Store and Dispose of Your Personal Data

The Company will store all preliminary personal data taken at interview and commencement of employment of Employees for the duration of the probationary period of 3 months. Once this time has lapsed all personal data no longer required ie DBS, photocopies of ID and financial information will be disposed of lawfully and according to correct procedures.

The Company will store an Employee's data for 6 years after the Employee has left the Company. Once this time has elapsed all electronic and paper copies will be disposed of lawfully and according to correct procedures.

The Company will store the personal data of applicants who have not been successful at interview for a period of 6 months after their initial interview. Once this time has lapsed all electronic and paper copies will be disposed of lawfully and according to correct procedures.

The Company will store a Resident's data for 6 years after the Resident has either left Camplehaye Residential Home or has become deceased. Once this time has lapsed all electronic and paper copies will be disposed of lawfully and according to correct procedures.

## How We Will Use Your Personal Data

We will only collect and process your Personal Data to the extent that it is needed to fulfil our operational and contractual needs or to comply with any legal requirements.

We shall access and use your Personal Data in accordance with your instructions and as is reasonably necessary:

- to fulfill our contractual obligations and responsibilities to you;
- to respond to your requests, queries and problems;
- **to** inform you about any changes to our services and related notices, such as security and fraud notices.

## When We May Share Your Personal Data

There are times when we may need to share your Personal Data. This section discusses how and when we might share your Data.

In the course of us fulfilling our role as your employer it will be necessary for us to disclose your Personal Data in certain situations:

- In our role as your employer we may need to share your Personal Data with certain bodies to fulfill our contract with you such as your training providers, the Company Accountants and HMRC.
- We use Care Control to process electronic data, including personal data. Care Control states that it is GDPR compliant and/or applies equivalent/adequate safeguards. It's privacy notice can be found here: https://carecontrolsystems.co.uk/gdpr/ and https://carecontrolsystems.co.uk/privacy-policy/
- We use secure external servers to process/store our electronic records, including your Personal Data which are maintained by Care Control.
- If we are under a duty to disclose or share your Personal Data in order to comply with any legal obligation, lawful requests, court orders and legal process.

- To enforce or apply any contract or other agreement with you.

- To protect our rights, property, or safety and that of our employees, members, or others, in the course of investigating and preventing money laundering and fraud.

## Access and portability requests

You are entitled to request access to your Personal Data unless providing a copy would adversely affect the rights and freedoms of others.

You can also request information about the different categories and purposes of data processing; recipients or categories of recipients who receive your Personal Data, details on how long your Personal Data is stored for, information on your Personal Data's source and whether the Data Controller uses automated decision-making.
You also have "Data Portability" rights which includes the right to request a copy of your Personal Data be sent to you or transmitted to another Data Controller.

## Correction requests

You are entitled to request we correct or complete your inaccurate or incomplete Personal Data without undue delay and we will update the information and erase or correct any inaccuracies as required. Rectification must take place within one month of your request for correction.

## Erasure requests

You can exercise your "right to be forgotten" and can request we erase your Personal Data. Once receiving a request we must erase the Personal Data without delay, unless an exception applies that permits us to continue processing your data. Details of such exceptions are contained in the Enactments and include situations where we might need to retain the information to carry out our official duties and/or comply with legal obligations and/or for the establishment of exercising or defending legal claims, or it is in the public interest to retain your Personal Data.

## Restriction requests

You may request restrictions be applied to the processing of your Personal Data for some specific reasons such as you contest the accuracy of the data, the processing is unlawful or if we no longer need to process your Personal Data. You can also request restrictions be applied if the processing is being done for public interest or third party reasons.
If such a request is received we can continue to store your Personal Data, but may only process it under certain circumstances, such as: you give consent for us to continue processing your data, we need to establish, exercise, or defend legal claims or we need to protect the rights of another individual or legal entity or for important public interest reasons.

## Objection requests

You may also object to your Personal Data being processed under certain circumstances, including for direct marketing purposes and profiling related to direct marketing.
If we receive such an objection we will stop processing your Personal Data unless we can show a compelling legitimate ground for processing your Personal Data which overrides your interests and the basis of your request.

## Your Telephone Queries and Requests

When receiving telephone enquiries, in which Personal Data is requested we will only verbally disclose Personal Data held on our systems if we can confirm the caller's identity so as to ensure that the data is only given to a person who is entitled to receive it.

We may suggest that a caller put their request in writing to assist in establishing the caller's identity, and to enable us to clearly record the nature of the request and to assist in further identity checks.

If we have reasonable doubts about the identity of the person making the request, we may request additional information to confirm the caller's identity.
In difficult situations our Data Users may refer a request to their line manager for assistance.

## Your Written Queries and Requests

When responding to written requests Personal Data will only be disclosed if we can confirm the identity of the sender and/or sufficient supporting evidence is provided by the sender establishing their identity.

## Responding to Your Requests

Upon receiving a request from you concerning your Personal Data, we will respond within one month of receiving the request by email (unless you request a response in an alternative format).
If we are unable to immediately comply with your request we will inform you within our response stating whether we need to extend our response time (for up to a maximum of two months), along with an explanation for the delay.

If we do not take any action within one month after receiving your request, you are entitled to request an explanation from us as to why no action was taken and you may make a complaint to the ICO: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow Cheshire SK9 5AF (Tel: 0303 123 1113) (email. casework@ico.org.uk)

When responding to Personal Data requests we will provide the information upon your payment of an administrative fixed fee of [£10]. Once the GDPR comes into force, we will not be entitled to charge for the provision of your personal data, unless the requests are manifestly unfounded or excessive, particularly if it is repetitive in which case we may refuse to act on the request, or apply further fees to cover the associated administrative costs.

## Breaches of Use of Personal Data

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Avens Care Homes Ltd must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Company must also inform those individuals without undue delay.

Avens Care Homes Ltd will ensure the Company have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not the Company needs to notify the relevant supervisory authority and the affected individuals.

Avens Care Homes Ltd will keep a record of any personal data breaches, regardless of whether the Company are required to notify.

## Your Complaints

If you feel that your questions or concerns regarding your Personal Data have not been dealt with adequately or that your request has not been fulfilled by us, you can use our complaints procedure, by emailing us at rebecca@avenscarehomes.co.uk

If, at the conclusion of our complaints procedure you do not feel that we have adequately dealt with your complaint you may make a complaint directly to ICO: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow Cheshire SK9 5AF (Tel: 0303 123 1113) (email. casework@ico.org.uk).

## Changes to our Data Protection Policy

We keep our privacy policy under regular review and reserve the right to amend and update the policy as required. Where appropriate, we will notify you of those changes upon request.

Signed:
Designation:
Date:
Review date: