

OAKWORTH MANOR CARE HOME LTD.	Issue Date: April 2019	Reviewed October 2026
	Next Review: 10/29	
<u>DATA PROTECTION POLICY</u>		

1. INTRODUCTION

- 1.1 This Data Protection Policy sets out how our Home handles the personal data of our residents, suppliers, employees, workers and other third parties.
- 1.2 You must read, understand and comply with this Data Protection Policy when processing personal data on our behalf and attend training on its requirements.
- 1.3 Personal data means any information about an individual from which that person can be identified.
- 1.4 Sensitive personal data includes 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, as well as personal data relating to criminal offences and convictions.
- 1.5 “Processing” means any activity that involves the use of personal data and 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.

2. SCOPE

- 2.1 All managers and departments are responsible for ensuring all workers comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.
- 2.2 The Data Security and Protection Lead **Ismar Alabedi** (DSPL), is responsible for overseeing this Data Protection Policy. Please contact the DSPL with any questions about the operation of this Data Protection Policy or the General Data Protection Regulation (GDPR) or if you have any concerns that this Data Protection Policy is not being followed.

3. PERSONAL DATA PROTECTION PRINCIPLES

- 3.1 We recognise the right of the individual resident to live the lifestyle of their choosing, subject to an appropriate Health & Safety Risk Assessment of the individual. Specifically, this Policy summarises the philosophy which recognises the right of the resident to have access to their personal files and/or case notes at any reasonable time:
- 3.2 We believe in the following:
 - 3.2.1 Records required for the protection of residents and for the effective and efficient running of the Home are maintained, are up to date and are accurate.
 - 3.2.2 Residents have access to their records and information about them held by the Home, as well as opportunities to help maintain their personal records.
 - 3.2.3 Individual records and Home records are kept in a secure fashion, are up to date and in good order; and are constructed, maintained and used in accordance with the GDPR and other statutory requirements.
- 3.3 We adhere to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

OAKWORTH MANOR CARE HOME LTD.	Issue Date: April 2019	Reviewed October 2026
	Next Review: 10/29	
<u>DATA PROTECTION POLICY</u>		

- 3.3.1 Processed lawfully, fairly and in a transparent manner.
- 3.3.2 Collected only for specified, explicit and legitimate purposes.
- 3.3.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- 3.3.4 Accurate and where necessary kept up to date.
- 3.3.5 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.
- 3.3.6 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.
- 3.3.7 Not transferred to another country without appropriate safeguards being in place.
- 3.3.8 Made available to data subjects who can exercise certain rights in relation to their personal data.

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

4. LAWFULNESS, FAIRNESS, TRANSPARENCY

4.1 LAWFULNESS AND FAIRNESS

- 4.1.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- 4.1.2 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.

The GDPR allows processing for specific purposes, for example:

- 4.1.3 the data subject has given consent;
- 4.1.4 to perform a contract with the data subject;
- 4.1.5 to meet our legal compliance obligations;
- 4.1.6 to protect the data subject's vital interests; or
- 4.1.7 to pursue our legitimate interests, provided that those interests are not overridden by the interests, fundamental rights and freedoms of the data subject which require protection of personal data.

4.2 CONSENT

- 4.2.1 A data subject consents to their personal data being processed if they indicate clear agreement either by a statement or some positive act. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document

OAKWORTH MANOR CARE HOME LTD.	Issue Date: April 2019	Reviewed October 2026
	Next Review: 10/29	
<u>DATA PROTECTION POLICY</u>		

which deals with other matters, then the consent must be kept separate from those other matters.

4.2.2 Data subjects must be able to withdraw their consent with ease 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 for processing, consent is usually required for processing sensitive personal data.

4.2.3 Please evidence any consents captured and keep records of all consents so that our homes can demonstrate compliance with consent requirements.

4.3 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

4.3.1 Whenever personal data is collected from data subjects, we must confirm in a Privacy Notice the identity of the data controller and the DSPL, as well as how and why we will use, process, disclose, protect and retain that personal data.

4.3.2 Where personal data is collected directly, this information must be presented when the data subject first provides the personal data.

4.3.3 Where personal data is collected indirectly (e.g. from a third party or a publicly available source), the data subject must be provided with all the information as soon as possible after collecting or receiving the data. Checks must also be made to ensure that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of it.

5. PURPOSE LIMITATION

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

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 cannot process personal data for any reason unrelated to your job duties. You should not collect excessive data. You must ensure that when Personal Data is no longer needed for specified purposes, 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.

8. STORAGE LIMITATION

Our Homes maintain retention policies and procedures to ensure that 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.

OAKWORTH MANOR CARE HOME LTD.	Issue Date: April 2019	Reviewed October 2026
	Next Review: 10/29	
<u>DATA PROTECTION POLICY</u>		

9. SECURITY INTEGRITY AND CONFIDENTIALITY

9.1 PROTECTING PERSONAL DATA

- 9.1.1 Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
- 9.1.2 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.
- 9.1.3 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, personal data. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.
- 9.1.4 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. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.
- 9.1.5 You must maintain data security by protecting the confidentiality, integrity and availability of the personal data.

9.2 Procedures

Staff should do the following:

- 9.2.1 Ensure that all files or written information of a confidential nature are stored in a secure manner in a locked filing cabinet and are only accessed by staff who have a need and a right to access them.
- 9.2.2 Ensure that all files or written information of a confidential nature are not left out where they can be read by unauthorised staff or others.
- 9.2.3 Care staff complete daily reports and review care plans. Residents and relatives are aware of the system and some are able to access the system personally.
- 9.2.4 Ensure that all care records and residents' notes, including care plans, are signed and dated.
- 9.2.5 Check regularly on the accuracy of data being entered into computers.
- 9.2.6 Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

9.3 REPORTING A PERSONAL DATA BREACH

We have put in place procedures to deal with any suspected personal data breach. If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DSPL. You should preserve all evidence relating to the potential personal data breach.

OAKWORTH MANOR CARE HOME LTD.	Issue Date: April 2019	Reviewed October 2026
	Next Review: 10/29	
<u>DATA PROTECTION POLICY</u>		

10. TRANSFER LIMITATION

- 10.1 The GDPR restricts data transfers to countries outside the European Economic Area (EEA) in order to ensure that the level of data protection afforded to individuals by the GDPR 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.
- 10.2 You may only transfer personal data outside the EEA if one of the following conditions applies:
- 10.2.1 the European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms;
 - 10.2.2 appropriate safeguards are in place such as binding corporate rules (BCRs), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DSPL;
 - 10.2.3 the data subject has provided consent to the proposed transfer after being informed of any potential risks; or
 - 10.2.4 the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

11. DATA SUBJECT'S RIGHTS AND REQUESTS

- 11.1 Data subjects have the right to:
- 11.1.1 withdraw consent to processing at any time;
 - 11.1.2 receive certain information about the data controller's processing activities;
 - 11.1.3 request access to their personal data that we hold;
 - 11.1.4 prevent our use of their personal data for direct marketing purposes;
 - 11.1.5 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;
 - 11.1.6 restrict processing in specific circumstances;
 - 11.1.7 challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
 - 11.1.8 request a copy of an agreement under which personal data is transferred outside of the EEA;
 - 11.1.9 object to decisions based solely on automated processing;

OAKWORTH MANOR CARE HOME LTD.	Issue Date: April 2019	Reviewed October 2026
	Next Review: 10/29	
<u>DATA PROTECTION POLICY</u>		

- 11.1.10 prevent processing that is likely to cause damage or distress to the data subject or anyone else;
 - 11.1.11 be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
 - 11.1.12 make a complaint to the Information Commissioner's Office; and
 - 11.1.13 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.
- 11.2 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).
- 11.3 You must immediately forward any data subject request you receive to the DSPL.

12. TRAINING AND AUDIT

- 12.1 You must undergo all data privacy related training and ensure your team undergoes similar mandatory training.
- 12.2 You must regularly review all the systems and processes under your control to ensure that they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

13. DIRECT MARKETING

- 13.1 We are subject to certain rules and privacy laws when marketing to our customers.
- 13.2 For example, a data subject's prior consent is required for electronic direct marketing (such as by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.
- 13.3 The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.
- 13.4 A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

14. SHARING PERSONAL DATA

- 14.1 Generally we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.
- 14.2 You may only share the personal data we hold with another employee, agent or representative of our Home or associated companies if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.
- 14.3 You may only share the personal data we hold with third parties, such as our service providers if:

OAKWORTH MANOR CARE HOME LTD.	Issue Date: April 2019	Reviewed October 2026
	Next Review: 10/29	
<u>DATA PROTECTION POLICY</u>		

- 14.3.1 they have a need to know the information for the purposes of providing the contracted services;
- 14.3.2 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;
- 14.3.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- 14.3.4 the transfer complies with any applicable cross-border transfer restrictions; and
- 14.3.5 a fully executed written contract that contains GDPR-compliant third party clauses has been obtained.

15. INTRODUCING NEW SYSTEMS AND PROCESSES

- 15.1 When introducing new systems and processes to the Home that involve processing personal data, a Data Protection Impact Assessment (DPIA) will be completed by the DSPL in conjunction with the Registered Manager. All new systems and processes should be discussed with the Registered Manager and DSPL before introduction.