

**OAKHAVEN CARE PRIVACY NOTICE
EMPLOYEES & JOB APPLICANTS**

Oakhaven is committed to maintaining the accuracy, confidentiality and security of your personal information. This Privacy Notice describes the personal information that we collect from or about you, how we use it and to whom we disclose that information.

Contents

Who we are 1

Who is responsible? 2

What personal information do we collect? 2

Why do we collect personal information? 3

How do we use your personal information? 4

What is our legal basis for collecting your data?..... 4

When do we share your personal information?..... 5

Who are our partner organisations?..... 6

How your records are stored 6

How is your personal information protected..... 6

How long is your personal information retained?..... 7

Updating your personal information 7

Right of access to your personal information 7

Your other legal rights 8

Monitoring 9

Website..... 9

Can we use your information for marketing our products and services?..... 9

Who to contact: 9

Changes to this privacy notice 10

Who we are

Oakhaven Care. Reg No: 08409572. Registered office: Lower Pennington Lane, Lymington, Hampshire, SO41 8ZZ.

We are committed to protecting your privacy and will only use personal data that we collect in line with all applicable laws, including the General Data Protection Regulation (GDPR). In this Notice, “We”, “Us” and “Our” means Oakhaven Care. “You” means the employee/job applicant. We are committed to maintaining the accuracy, confidentiality and security of your personal information. Data protection law provides you with a right to be informed about the processing of your personal information. This Notice describes the personal

information that we collect from or about you, and how we use and to whom we disclose that information.

Where it is appropriate to the delivery of the service and in accordance with our contract with you or as required by law, we may also prescribe additional purposes and longer retention periods to those set out below.

Who is responsible?

The person responsible for the personal information about you which we collect (the “data controller”) is Oakhaven.

What personal information do we collect?

We will collect, store, and use the following categories of personal information about you:

- Personal and contact details (name, title, address, phone, email)
- Date of birth and gender
- Next of kin and emergency contacts
- Bank account and payroll information
- Employment details (start date, workplace, role)
- Identification documents (driving licence, passport, right to work checks)
- Recruitment information (CVs, references, application materials)
- Performance, disciplinary, and grievance records
- Use of company information and communication systems

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

For the purposes of this Privacy Notice, personal information is any information about an identifiable individual. Personal information does not include anonymous or non-personal information.

We collect and maintain different types of personal information in respect of those individuals who seek to be, are, or were employed by us, including the personal information contained in:

- CVs and applications;
- references and interview notes;
- DBS and vetting information;

- Education and training information;
- Right to work information;
- Photographs, testimonials, video and audio recordings including cctv imagery;
- letters of offer and acceptance of employment and other employment records;
- policy acknowledgement sign-off sheets;
- payroll information; including but not limited to national insurance number, banking and deposit information and national insurance number;
- wage and benefit information including annual leave information;
- forms relating to the application for welfare benefits;
- Health questionnaires and risk assessments including details of any medical condition or medication you are taking, including vaccination records;
- beneficiary and emergency contact information;
- Disciplinary and grievance records;
- Your driving licence and insurance documentation; and
- Equal opportunities monitoring forms

In addition to the examples listed above, the personal information we collect includes information such as your name, home address, telephone, personal email address, date of birth, employee identification number, ethnicity, marital status, nationality, next of kin/emergency contact information, salary, biometric data provided and any other information necessary for business purposes, which is voluntarily disclosed in the course of an employee's application for and employment with us.

The above lists are non-exhaustive and applies across the organisation.

As a general rule, we collect personal information directly from you. We may however also use recruitment consultants and recruitment websites to source potential applicants. In most circumstances where the personal information that we collect about you is held by a third party, we will only process it in accordance with our legitimate interests, where necessary for the performance of our contracts or where obligated by law.

Where permitted or required by applicable law or regulatory requirements, we may collect information about you without your knowledge or consent.

Why do we collect personal information?

The personal information collected is used and disclosed for our business purposes, including establishing, managing or terminating the employment relationship and complying with our obligations to you. It is necessary for the performance of our contract with you and/or performing our obligations under a contract as well as to meet our legal obligations and legitimate interests. In respect of special category data, which includes health data, it is necessary for your employment, social security and social protection, reasons of substantial public interest and/or for reasons of public interest in the area of public health, such as protecting against serious threats to health. Such uses include:

- Assessing eligibility and suitability for employment, including recruitment checks, references, and qualifications.

- Administering pay, benefits, and work-related claims.
- Identifying training, development, performance, and promotion requirements.
- Managing disciplinary, grievance, and whistleblowing processes.
- Maintaining emergency contact details and ensuring health, safety, and wellbeing.
- Monitoring equality, diversity, and pandemic or infection control requirements.
- Complying with legal, regulatory, and contractual obligations.
- Compiling internal contact lists and analysing workforce trends.
- Protecting the security of staff, premises, and company information.
- Any other purposes reasonably necessary for employment, safeguarding vital interests, or performing tasks in the public or legitimate business interest.

How do we use your personal information?

We may use your personal information for the purposes described in this Policy, or for any additional purposes that we advise you of and, where your consent is required by law, where we have obtained your consent in respect of the use or disclosure of your personal information.

We may use your personal information without your knowledge or consent where we are permitted or required by law or regulatory requirements to do so.

What is our legal basis for collecting your data?

We collect, store, and use your personal information based on the following legal grounds under the UK GDPR:

Performance of a Contract

Processing your information is necessary to fulfil our employment contract with you. This includes administering payroll, benefits, holidays, training, and managing your role and responsibilities.

Legal Obligation

We process certain personal data to comply with laws and regulations. Examples include statutory payroll reporting, tax obligations, safeguarding requirements, health and safety, and regulatory reporting to bodies such as HMRC, the Charity Commission, and the HSE.

Legitimate Interests

We process personal information where it is necessary for our legitimate interests, provided that your rights and freedoms are not overridden. Examples include managing the workforce, improving HR processes, monitoring IT systems for security, and protecting our property and staff.

Consent

In limited cases where processing relies on consent (e.g., marketing communications or participation in optional surveys), you can freely give, withdraw, or update your consent at any time. Withdrawing consent will not affect the lawfulness of processing carried out before you withdrew it.

Vital interests

Where necessary to protect your life or the life of another person, we may process personal data without your consent, for example in emergencies involving health or safety.

Special Category Data (Sensitive Data)

For processing sensitive information, such as health, trade union membership, or ethnicity, we rely on additional grounds permitted under UK GDPR, including:

- Employment law obligations and social security or social protection purposes
- Protecting vital interests, where you are physically or legally unable to give consent
- Substantial public interest, such as health and safety, equal opportunities, or pandemic monitoring

We will always use the minimum personal information necessary for these purposes and ensure it is processed securely and only for the stated purposes.

When do we share your personal information?

We may share your personal information with our employees, clients, contractors, advisers or consultants and other parties who require such information to assist us with establishing, managing, funding or terminating our employment relationship with you, including: professional advisers, parties that provide products or services to us or on our behalf and parties that collaborate with us in the provision of products or services to you.

Also, your personal information may be disclosed:

- as necessary for the performance of our contract with you
- as permitted or required by applicable law or regulatory requirements. In such a case, we will try to not disclose more personal information than is required under the circumstances;
- to comply with valid legal processes such as warrants or court orders;
- as part of our regular reporting activities to our clients or other members of the organisation, i.e. if necessary for the performance of your contract, to comply with a legal obligation or as part of our legitimate business interests;
- to protect the rights and property of the company or others;
- during emergency situations or where necessary to protect the vital interests or safety of a person or persons;

- to assess your working capacity;
- if in the substantial public interest;
- where the personal information is publicly available; or
- with your consent.

Who are our partner organisations?

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations:

- HR platforms (e.g. CIPHR, I-Rota) – to receive and store employee data and manage employment relationship and processes.
- Payment processors (e.g. Intacct & CIPHR Payroll) – to process salary payments securely.
- Benefit system providers – to store and process employee benefits (e.g. Scottish Widows, BUPA, Unum, NHS Pensions).
- Regulators or legal authorities (Charity Commission, HSE, DBS HMRC) — where legally required.
- Occupational health providers or medical practitioners – to assess fitness for work, workplace adjustments or health related support.
- HR consultants – to provide independent advice and support during formal HR processes such as disciplinary, grievance, capability, or absence management cases.
- Other ‘data processors’ which you will be informed of

You will be informed who your data will be shared with and in some cases asked for explicit consent for this happen when this is required.

How your records are stored

We store employee information primarily in a secure electronic HR database (CIPHR) and rostering system (PeoplePlanner). This system is used to manage employee data and processes. Access to employee information is strictly limited to staff who need it to carry out their roles, and is controlled through secure login, permissions, and regular monitoring.

We also use secure IT systems and encrypted storage to protect information that may be held in other formats (for example, financial transaction records or paper documentation that you provide to us), and we ensure that all personal data is handled in line with data protection legislation and our internal policies.

How is your personal information protected?

We endeavour to maintain physical, technical and procedural safeguards that are appropriate to the sensitivity of the personal information in question. This includes the use of firewalls and encryption as well as other information security requirements, systems and procedures. These safeguards are designed to protect your personal information from loss and unauthorised access, copying, use, modification or disclosure.

We also use data sharing agreements, data processing agreements and the standard contractual clauses to protect your data where it is being shared, processed and/or transferred to a third country.

How long is your personal information retained?

For unsuccessful job applicants or those who do not accept a position with us, we will generally destroy your data after 6 months unless you have requested that we retain it for longer.

For recruited staff, except as otherwise permitted or required by applicable law or regulatory requirements, we will only retain your personal information for as long as we believe it is necessary to fulfil the purposes for which the personal information was collected (including, for the purpose of meeting any contractual, legal, accounting or other reporting and regulatory requirements or obligations). We may, instead of destroying or erasing your personal information, make it anonymous such that it cannot be associated with or tracked back to you. In most cases your data will be deleted 6 years after you have left the company or as otherwise set out in accordance with our data retention schedule and/or as required by law.

Retention of Special Category Data

Special category data, such as health information, ethnicity, and trade union membership, is retained only as long as necessary for employment purposes, or to comply with legal obligations. In most cases, employee special category data is retained for the duration of employment plus 6 years after leaving the organisation, unless longer retention is required by law.

Updating your personal information

It is important that the information contained in our records is both accurate and current. If your personal information happens to change during your relationship with us, please keep us informed of such changes.

You have a right to have your personal information corrected if it is inaccurate and to have incomplete personal information completed. In some circumstances we may decide to update our record of your personal information by appending additional text without deleting the original record. We would advise that you raise any changes with us as soon as they occur so that the data we keep about you is kept up to date.

Right of access to your personal information

You can ask to see the personal information that we hold about you. If you want to review, verify or correct your personal information, please contact Oakhaven. Please note that any such communication may be required in writing.

When requesting access to your personal information, please note that we may request specific information from you to enable us to confirm your identity and right to access, as well as to search for and provide you with the personal information that we hold about you.

You have the right to access the personal information we hold about you. In most cases, we will provide this information upon request. However, in limited circumstances, applicable law or regulatory requirements may allow or require us to withhold certain information. This may include:

- Personal information that has been destroyed, erased, or anonymised in line with our record retention policies
- Information where disclosure is restricted by legal or regulatory obligations

If we are unable to provide full access to your personal information, we will explain the reasons for this wherever possible, subject to any legal or regulatory restrictions.

Your other legal rights

Data protection legislation also provides you with certain other rights. These are not always absolute rights and must be considered in the wider scope of the legislation. These rights are:

| | |
|--|---|
| <u>Right of access and of data portability.</u> | You have the right of access to information we hold about or concerning you and/or to have it transferred to another data controller in some circumstances. If you would like to exercise this right, you should contact our Data Protection Officer. |
| <u>Right of rectification or erasure.</u> | If you feel that any data that we hold about you is inaccurate you have the right to ask us to correct or rectify it. You also have a right to ask us to erase information about you where you can demonstrate that the data we hold is no longer needed by us, or if you withdraw the consent upon which our processing is based, or if you feel that we are unlawfully processing your data. Your right of rectification and erasure extends to anyone we have disclosed your personal information to, and we will/shall take all reasonable steps to inform those with whom we have shared your data about your request for erasure. |
| <u>Right to restriction of processing.</u> | You have a right to request that we refrain from processing your data where you contest its accuracy, or the processing is unlawful and you have opposed its erasure, or where we don't need to hold your data anymore but you need us to in order to establish, exercise or defend any legal claims, or we are in dispute about the legality of our processing your personal data. |
| <u>Right to object.</u> | You have a right to object to our processing of your personal data where the basis of the processing is our legitimate interests including but not limited to direct marketing and profiling. |
| <u>Right to Withdraw Consent.</u> | You have the right to withdraw your consent for the processing of your personal data where the processing is based on consent. To withdraw consent please <i>select the unsubscribe option in the</i> |

| | |
|----------------------------|---|
| | <p>most recent electronic marketing communication you have received or alternatively you can write to us at dataprotection@oakhavenhospice.co.uk</p> |
| Right of Complaint. | <p>You also have a right to lodge a complaint about any aspect of how we are handling your data with the UK’s Information Commissioner’s Office who can be contacted at www.ico.org.uk.</p> |

Monitoring

Some of our premises are equipped with CCTV. Where in use, CCTV cameras are there for the protection of visitors and employees, and to protect against theft, vandalism and damage to goods and property on the premises. Generally, recorded images are routinely destroyed after 30 days and are not shared with third parties unless there is suspicion of a crime, in which case they may be turned over to the police or other appropriate government agency or authority.

This section is not meant to suggest that individuals will be monitored or their actions subject to constant surveillance. It is meant to bring to your attention the fact that such monitoring may occur.

Website

When you use our website, we use tools like Google Analytics to collect information such as your IP address, the browser you use (e.g. Internet Explorer, Firefox etc.), domain names, the time of day you accessed the website and referring Website addresses. This information helps improve our online services, ensures security and helps protect against fraud. It also assists with diagnosing online problems with our website. We also use cookies to give us more understanding of how people use our website.

Details on how you can manage your cookie settings can be found at: [Cookie policy - Oakhaven](#)

Can we use your information for marketing our products and services?

We may send you email newsletters if you opt-in to receive such correspondence. We may also send you details of new services but only if it is within our legitimate interest to do so. We will always let you know that you can opt out from receiving marketing material and you can let us know at any time if you no longer wish to receive direct marketing offers from us. You can do so by emailing us at fundraising@oakhavenhospice.co.uk.

Who to contact:

Oakhaven Care has the responsibility to ensure that your personal data is protected. If you have any complaints or concerns, we advise that you contact us initially before raising this with the ICO.

We recommend that you contact the data protection officer below:

Privacy Notice – Employees & Job Applicants

Name of Person: Donna Wilkins, Data Protection Officer
email address: dataprotection@oakhavenhospice.co.uk
Contact number: 01590 613030
Contact address: Oakhaven Hospice, Lower Pennington Lane, Lymington, SO41 8ZZ

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance.

Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/> or call 0303 123 1113.

Changes to this privacy notice

Rules and regulations around data can change – and therefore our privacy notice will change too. So, it's worth visiting this page from time to time to check for updates. At the bottom of this privacy notice we tell you when it was last updated.