**PRIVACY POLICY**

**What we process**

Elder Healthcare process personal data about enquirers, residents, and individuals during and after their contact with us. This processing is required to support our business interests and to fulfil our legal and contractual obligations that are compliant with The UK & EU General Data Protection Regulation (UK GDPR) (EU GDPR), UK Data Protection Act 2018 (DPA2018) and Caldicott Principles including guidance from the 10 data security standards, which include:

- Providing services to our enquirers, residents, and individuals we support, recording what services we have provided;
- Managing the health, welfare, safety and security of our residents and individuals we support;
- Handling enquiries, complaints, and investigations;
- Monitoring and improving the quality of our services;
- Using Legitimate interests for researching and understanding the needs of our target audience and to improve our marketing effectiveness;
- Working with our partners such as recruiting sites and providers to improve the quality of our services.

We also process personal data about job applicants, current and former employees, service providers, and other groups of individuals during our business operations, and this data is subject to our internal privacy policies.

Personal data you provide to us

We collect personal data you provide to us when you enquire, work in, or use any of our services, for example:

- **Enquiry:** Personal details (name, gender, age etc.), contact information (home address, phone number, email address etc.), details of your interests and communications preferences;
- **Residents:** Personal details, contact information, financial details, relative, or next of kin, care needs;
- **Complaints:** Personal details, contact information, enquiry, or complaint details;
- **Health & Welfare:** Medical, dietary and mobility details provided to us before, during or after any stay with us in one of our services;
- **Job Applications:** Responses to Job applications, including contact details, CV's and other personal information provided.

Data anonymisation and use of aggregated information

Your information may be converted into statistical or aggregated data in such a way as to ensure that you are not identified or identifiable from its content. This aggregated data cannot be linked back to you as an individual. The methods used to protect this data is encryption, pseudonymisation and anonymisation.

We may share your information with:

When you are a resident in one of our services with;

- A sponsor to organise payment of fees.
- Your next of kin or named family member.
- Any person that you have appointed to act on your behalf pursuant to a valid Power of Attorney or allied professionals and other health care providers in the case of an emergency.

or with;

- Organisations and consultants providing contracted services to us (for example, information technology service providers who provide and maintain our systems and our website hosting). Where these companies and consultants do provide services to us, we will only use your information in compliance with the UK & EU General Data Protection Regulation, UK Data Protection Act 2018, and the Caldicott Principles.
- The courts in the United Kingdom or abroad as necessary to comply with a legal requirement, for the administration of justice, to protect vital interests and to protect the security or integrity of our business operations.
- A third-party company, for example when providing a reference for a former employee, or if a resident who transfers to another service provider. This transfer of data would only take place in accordance with strict compliancy criterion which is transparently conducted.

Where we store your information

We only store your information on servers stored off site. These servers are fully protected and encrypted.

As part of our process, we carry out and document full Data Protection Impact Assessments on systems and implement changes based on its outcomes.

Retention of your information

Residents:

- If you participate in any pre-admission assessment but do not go on to become a resident within Elder Healthcare, we will only keep your information for as long as it is lawfully necessary to enable compliance with our legal and contractual obligations and any related legislations.
- If you become a resident at a Elder Healthcare, we will keep your information for as long as you continue to be a resident, and then depending on certain circumstances, for 7 years after your contract has ended.

- All the information we hold is secured, kept confidential and protected with the use of strict processes and policies such as access restrictions and encryption that are in line with UK & EU GDPR, DPA2018 and the Caldicott Principles

Job Applicants
Information provided by candidates that are unsuccessful in their application for employment, such as CV's, shall be securely deleted after 12 months, unless we are given permission to keep the data for a longer period.

Your rights

- You have enhanced rights under the new act in respect of the information we hold subject to some exemptions.

Please note that the way we process your information and the legal basis on which we rely on to process it affects the extent to which these rights apply.

These rights are the:

- Right to **be informed** about the processing of your information (this is what this notice sets out to do);
- Right to have your information **corrected if it is inaccurate** and to have **incomplete information completed**;
- Right to **object to processing** of your information;
- Right to **withdraw your consent** at any time where we rely on it to process your information;
- Right to **restrict processing** of your information;
- Right to have your information **erased**;
- Right to **request access** to your information and information about how we process it;
- Right to **move, copy or transfer** your information; and
- Right to **automated decision making**, including profiling.

If you would like to discuss or exercise any of these rights, please contact us using the details provided both at the top and bottom of this Privacy Policy.

Where you believe your information has or is being used in a way that you believe does not comply with data protection law. You have the right to lodge a complaint with the Information Commissioner's Office. We encourage you to contact us before making any complaint and we will seek to fully resolve any issues or concerns you may have.

You can also contact our Data Protection Officer,

Kirsty Harrison-Quinney – DPO for Elder Healthcare – kirsty@elderhealthcare.im

Why are we collecting your information?

The information that you provide to us as part of your application will be used by us to assess your suitability for the job for which you are applying.

Type of personal information we use

We are collecting information about you which is relevant to our consideration of your application for employment. This includes:

- Personal details (such as name, date of birth, gender, marital status, national insurance number);
- Contact details (such as your address, personal telephone number and personal email address);
- Confirmation of your identity (such as a copy of your driving license);
- Recruitment information (such as copies of right to work documents, references and other information included in a CV or cover letter or as part of the application process); information about your family and others (such as dependents, next of kin and emergency contact numbers); information about your previous employment (such as job titles, work history, working hours, training records, professional memberships, disciplinary information / compensation history); and any other information you provide to us during an interview.

**Special categories of personal data**
Some of the information which we collect may be specified under UK & EU GDPR as "special categories of personal data", and as such require a greater level of protection.

If we are required to collect this category of data, you will be informed of the specific reason why this is required. Where there is a legal obligation to collect such information, this will be clearly stated at the time of collection.

Where will we obtain this information?

As part of the recruitment process we may obtain information from:

- YOU directly as part of the recruitment process.
- Employment agencies.
- Job boards such as Reed and Indeed.
- Background check providers;
- Former employers / referees;

How we will use your personal data during the recruitment process

**How your information may be used**

- Assessment – to assess your skills, qualifications and suitability for the role you have applied for
- Contract – It is necessary in order for us to take steps to enter into a contract with you.
- Legal obligations – It is necessary to meet legal / regulatory obligations
- Employment – It is necessary for us to carry out our rights and obligations as your potential employer
- Communication – to communicate with you during the recruitment process;

- Records – to keep records of our hiring processes
- Monitoring – to comply with our legal obligations such as to prevent fraud and equal opportunities monitoring. Legal obligations: It is necessary to meet legal / regulatory obligations
- Adjustments – to consider whether we need to provide appropriate disability adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview, to comply with our legal obligations as an employer and where it is needed in the public interest (such as equal opportunities monitoring)
- Health – It is necessary to assess the working capacity of potential employees

How we use information about criminal convictions

We have a duty of care to ensure the people we employ have no history that would indicate they are unsuitable to work with vulnerable people. Where appropriate we will collect information about criminal convictions as part of the recruitment process such as background and reference checks, these may include:

- Disclosure and Barring Service check
- Checking you are legally entitled to work in the UK

*(We will use information about criminal convictions and offences to assess whether you are a fit and proper person to work for us, and to protect our vulnerable people from assault, abuse, theft of possession or any other detriment at the hands of unsuitable employees)*

We are allowed to use your personal information in this way to carry out our obligations as your potential employer and because it is necessary to meet legal / regulatory obligations.

Complying with data protection law

**Sharing your Information**

We will only share your personal information with third parties where we are required to do so by law, or where there is a legitimate interest in doing so.

**Which third-party service providers process my personal information?**
As a "Data Controller" (legal term under the UK Data Protection Act 2018) we are required to ensure that we only share data with third parties who fully meet the requirements of the UK Data Protection Act 2018. These third parties are Called "Data processors" and we will only share data with them, if they are fully compliant.

Can we use your information for any other purpose?

We typically will only use your personal information for the purposes for which it was originally collected. Should we require to use it for other purposes, where we do not have a legitimate interest, we will seek your permission first.

Storing your information and deleting it

If your application is unsuccessful we will only retain your personal information for as long as is necessary to fulfil contractual obligations with you, such as legal, accounting, or reporting

requirements, for a maximum period of 12 months. You have rights under the UK Data Protection Act 2018 to ask us to delete this earlier if required.

Your Rights

We mention that you have new rights under the UK Data Protection Act 2018, these include:

- **The right to be informed**: Organisations need to tell individuals what data is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties. This information must be communicated concisely and in plain language.
- **The right to access**: Individuals can submit Data Subject Access Request which oblige organisations to provide a copy of any personal data concerning the individual. Organisations have one month to produce this information, although there are exceptions for requests that are manifestly unfounded, repetitive or excessive.
- **The right to rectification**: If the individual discovers that the information an organisation holds on them is inaccurate or incomplete, they can request that it be updated. As with the right to access, organisations have one month to do this, and the same exceptions apply.
- **The right to erasure** (also known as 'the right to be forgotten'): Individuals can request that organisations erase their data in certain circumstances, such as when the data is no longer necessary, the data was unlawfully processed or it no longer meets the lawful ground for which it was collected. This includes instances where the individual withdraws consent.
- **The right to restrict processing**: Individuals can request that organisations limit the way an organisation uses personal data. It's an alternative to requesting the erasure of data, and might be used when the individual contests the accuracy of their personal data or when the individual no longer needs the information but the organisation requires it to establish, exercise or defend a legal claim.
- **The right to data portability**: Individuals are permitted to obtain and reuse their personal data for their own purposes across different services. This right only applies to personal data that an individual has provided to data controllers by way of a contract or consent.
- **The right to object**: Individuals can object to the processing of personal data that is collected on the grounds of legitimate interests or the performance of a task in the interest/exercise of official authority. Organisations must stop processing information unless they can demonstrate compelling legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual or if the processing is for the establishment or exercise of defence of legal claims.
- **Rights related to automated decision making including profiling**: The UK Data Protection Act includes provisions for decisions made with no human involvement, such as profiling, which uses personal data to make calculated assumptions about individuals. There are strict rules about this kind of processing, and individuals are permitted to challenge and request a review of the processing if they believe the rules aren't being followed.

Data protection contacts

If you have any comments, complaints or suggestions in relation to our notice or even the way we process information about you, please contact our Data Protection Officer, Kirsty Harrison-Quinney at kirsty@elderhealthcare.im

Elder Grange Nursing Home

Fuchsia Lane

Governors Hill
Douglas

Isle of Man – IM2 7EB

Telephone: 01624 626282