Privacy Notice – Residents & Customers

This document sets out what information The Manor House Care Home collects about the residents, their families or those with power of attorney, how it uses the information, how it protects the information and your rights.

The Manor House Care Home, is committed to ensuring your privacy is protected in accordance with Data Protection Standards.

The Manor House Care Home, is using the following definition for personal data:

Personal data	*Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.* *Personal data we gather may include: individual's contact details, educational background, financial/credit worthiness and pay details, details of certificates and diplomas, education and skills, job title, and CV.*
Sensitive personal data	*Personal data about an individual's racial or ethnic origin, marital status, nationality, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings. Any use of sensitive personal data will only ever be carried out with the express permission of the individual.*

The Manor House Care Home, may change this policy from time to time by updating this page. This policy is effective from 28th May 2018. Any updates or changes to the use of your personal data will be advised to you, prior to that change of use.

What this Privacy Notices relates to

This privacy notice relates to our client assessment, engagement and ongoing care and support services.

Who We Are?

The Manor House Care Home, Fore Street, Seaton, Devon, EX12 2AD, United Kingdom

Contact Us.

Web Address: https://www.manorhouse-seaton.co.uk

Email : hutchc@strngarm.demon.co.uk

Phone : 01297 22433

Post: The Manor House Care Home, Fore Street, Seaton, Devon, EX12 2AD, United Kingdom

Your Rights

Under the Data Protection Law (GDPR & E-Privacy) you have a number of rights.
These are:

Right to Confirmation and Access

You have the right to confirm what personal data is being held and to what purpose it is being used.
You have the right to obtain copies of the personal data that is being held about you.
You have the right to obtain confirmation of the safeguards being implemented with regards any sharing of your personal data with third parties.

Right to Be Forgotten (Right to Erasure)

You have the right to have information about you to be irretrievably erased. Where legal for us to do so, where it does not interfere with our ability to provide any ongoing services to you and so long as your request does not involve the interference of the personal data of another person, we will when requested:
1. Ensure the prompt erasure of that data within a reasonable amount of time – which you will be informed of
2. Issue the instruction to any third-parties, where they are acting as a processor on our behalf, to do the same

We will keep a minimum record of this request detailing:
1. Who you are (name, email address and what supporting documentation was used to verify your identity)
2. When you asked for the action to be undertaken
3. What action you asked to be undertaken
4. When the action was undertaken

This information is necessary to protect both you and the company and so we are recording this minimum information on the basis of legitimate interest.

Subject Access Request

You have the right to request the nature and actual information that we hold about you and we are required to:
1. Inform you of the data we hold on you
2. Inform you of the data you have agreed for us to share with third-parties and who those third parties are

3. Have information requested on your behalf e.g. through a solicitor or a person with power of attorney or similar authority

Under usual circumstances we will ensure that we comply with the current law and provide this information to you within 30-days.
However, where there are large volumes of information or the request is complex we may be required to contact you for clarification. In the event of a complex request we will inform you of the likely timescale. In the event you are not satisfied with this you also have the right to complain by contacting us at the address set out in the contact details on page one of this document.
To complete a subject access request (SAR), please contact us at the address set out on page one of this document. You will be required to verify your identity appropriately before we release any personal data this may require us to undertake further identify checks against you/the information you have provided.
All subject access requests shall be recorded on our internal log.

The Right to Object to Automated Decision Making or Profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling. You will however, be informed in the relevant privacy policy of any automated decision making or profiling.

Right to Object to Processing

You have the right to object, on grounds relating to your situation, at any time, to the processing of personal data concerning you. However, you will be made aware of the consequences of any objection at the time it is raised.

The Right to Rectification

Where at all possible we will provide you direct access to update, correct and generally maintain your own information. We do this because you are more likely to be aware of changes to your information than we are. That said, we are also under an obligation to ensure that the personal information we have about you is correct in the event you are not able to update this yourself. In the event that information changes please inform us of these changes by contacting us at the address set out on page one of this document and we will endeavour to update your personal information within 48-hours (mon-fri). Certain updates where they coincide with third party systems e.g. banking, may be withheld to ensure that there is reduced chance of corruption.

Withdrawal of Consent and/or Limit Processing

In the event that we are using your personal data with your consent, you can withdraw that consent at any time.
You can do this by contacting us directly.

In some case's you may not want to entirely withdraw consent but limit the breadth of processing we undertake using your data. The extent to which we process your data will be provided in the relevant privacy policy for the service(s) we are providing you. Some processing is necessary in order that we can deliver that service, any impact on this will be explained to you in the event you wish to limit processing. That said you can always contact us at the address set out on page one of this document, to discuss this.
The legal basis for processing will be explained to you in the specific privacy policy for that service.

Right to Data Transfer

Some of our services use systems that allow us to export data in common formats such as comma separated values (csv) files, spreadsheets etc.
In the event that we are providing services that allow this type of export, you have the right to request that this information is exported and provided to you or another supplier of such services.
You will be required to provide the same identify verification information in the same manner as the subject access request.

Right to Complain

If at any time you feel that we have failed to safeguard your information appropriately you have the right to complain.
In the first instance we would ask you to contact us and allow us to investigate and identify any issues you may have, by contacting us:
On-Line : https://www.manorhouse-seaton.co.uk
Email : hutchc@strngarm.demon.co.uk
Phone : 01297 22433
Post: The Manor House Care Home, Fore Street, Seaton, Devon, EX12 2AD, United Kingdom

You do however have the right to complain directly to the appropriate regulatory authority in your country, place of work or where you believe any issue has occurred.

In the case the UK, the regulatory authority is the Information Commissioners Office (ICO) and they can be contacted here:
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom. Phone: +44 (0) 303 123 1113, Email: casework@ico.org.uk.
Website: https//ico.org.uk.

Security

All Employees are responsible for ensuring that any personal data that The Manor House holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by The Manor House to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security and must be kept:
o in a lockable room with controlled access; and/or
o in a locked drawer or filing cabinet; and/or
o if computerised, held on password protected computer systems

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of The Manor House

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with data retention. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site. Staff must be specifically authorised to process data off-site.

Where at all possible we encrypt all information that is either stored or transmitted to third-parties. Where data is stored or transmitted to a Third Country (any country outside of the European Economic Area (EEA)) we will ensure appropriate adequacy protection is in place in accordance with Data Protection Legislation.
Consequently, we may also need to sometimes undertake further security and screening questions when undertaking our routine dealings with you these are there to protect your personal data and security. Whilst we undertake all reasonable precautions, encryption, software updates and patches, we cannot guarantee the safety of data transmitted over the internet.

Data Breach

In the event of a data breach of your personal data, which means:
"The unintended loss, destruction amendment or disclosure of personal data"

We will first do all that is necessary in order to minimise the impact on you, identify any potential malicious third-party, identify any third-parties that may also be impacted and take all reasonable efforts to ensure that you are notified.
In the event that we are notified by a third-party of a breach, in their systems, we will undertake the same level of efforts.
We will undertake this communication either directly with you as an individual or by sending out a public notification.

At the same time, we will comply with the current law in respect of informing the appropriate supervisory authority which is currently the Information Commissioners Office (ICO). We are under a legal requirement to report data breaches to the ICO.

What Personal Data are we collecting?

To ensure that we can process your application for care and support services with us, we will be processing the following information:

- Your full name, address and contact details and next of kin information.
- Your capacity to make decisions and/or whether we need to liaise with the person(s) you have entrusted with power of attorney.
- Any specific medical conditions that may affect our staff, other residents and our ability to look after you.
- Any specific health issues that you may be required to disclose, depending on the nature of the care we will be providing you.
- Details relating to the methods through which your care is being funded. If you are funding your care, then we will take payment through standing order or direct debit. If your care is being funded, then we will deal with the organisation funding this, or any other party that you have nominated or has agreed to pay for your care.
- We will record details of any medication you require in order that we can ensure we administer this and we will also record any specific medical care wishes you have.
- If you wish us to, we will record other information such as your religion to allow us, at your request, to contact the appropriate religious representative.

Are we likely to need any Sensitive Personal Data?

Yes. In order to ensure that we can provide the necessary care to you as an individual, to ensure that we can protect our staff and other residents and potentially to make an assessment of whether we are able, at all to provide the care you need, we need to understand aspects of your care needs such as medical, physical, psychological and mental wellbeing.

In some cases, we will also ask about communicable diseases or other conditions that may put you, other members of staff or our clients at any risk. We will only ask for this information if it is necessary and you will be made aware of this in the assessment process.

In the event you are unwell this information will be passed onto medical professionals e.g. ambulance, GP, hospital services.

Why we need this information?

We need this information to:

1. Fulfil our contract with you. Providing your care services at the start of your time with us as well as adapting those services as your needs change.

2. In medical situations. To ensure that we have the necessary medical information about you to be able to pass onto medical professionals in the event you are incapacitated.

3. To comply with the law and government defined care service regulations and/or standards such as those regulated and inspected by the Care Quality Commission.

4. If you are the next of kin or person with power of attorney, then your details are required to ensure that we can get the necessary authority in respect of the care services we are providing to the person under your authority.

What is the legal basis of processing?

We will only ask for information relevant to the service(s) we are providing you in order to: deliver those services to you; to comply with your wishes; or to 'protect life'. Subsequent processing will only be carried out where it is appropriate or where we are legally obliged to as part of our industry compliance requirements, where we are providing you a benefit by way of your contract or where we need to protect the interests of the company. You will be informed of any processing or sharing of data before it is shared.

The legal basis of processing your personal information is explained below:

Legal Basis	Explanation	Examples
Contractual Obligation	When we have a contract with you to provide care and/or support services.	Providing residential care and/or nursing care.
		Administering your medication

Legal Basis	Explanation	Examples
Legal Obligation	This is where the organisation has a legal obligation to comply with current law, industry compliance requirements, court order etc.	Providing funding agencies with information about the services we are providing you, in the event that they are paying for those services.
		To comply with the Health & Social Care Act and the Care Quality Commission Standards.
		Where we are required to be able to demonstrate skills and competences of our staff to comply with industry or legal requirements.
Vital Interest	Where the collection or sharing of information is in the vital interest to you or other members of the public, including staff or clients.	Obtaining your next of kin details.
		Sharing appropriate identity/ information with a medical provider (ambulance, doctor, hospital etc.) in the event you are taken ill.
		Where your condition may represent a threat to the interests, rights and freedoms of other people e.g. if you have a communicable disease and we believe your condition may represent a risk to other residents.

Legal Basis	Explanation	Examples
Consent	Where the processing or sharing of your information is based on you explicitly consenting to such sharing or processing.	Sharing your information with a religious representative.
		Sharing your information with a third-party service e.g. chiropodist, hairdresser.
		Using your imagery for social media, website or other marketing material.

How do I withdraw consent or change my preferences?

You can object to us processing your data at any time by:

1. Informing the care team
2. By contacting us and letting us know what you would like to change

Be aware that in some cases, objecting to the processing or sharing of your information may result in a service being withdrawn or us being unable to comply with the law or our contract with you. You will be informed of how we can or cannot comply with your request, when/if you were to make such a request.

What decisions are going to be made using my personal data?

The primary decision made relating to your personal data is whether we can initially or during your stay with us, continue to provide the necessary care services you require. Whether your stay with us is short-term or long-term.

These decisions will be based on your medical, physical and psychological needs, both initially and during your stay with us.

It may be necessary for us to obtain alternative authority, such as from a member of your family with power of attorney, if you become unable to make certain decisions yourself. In this event, we will continue these assessments involving those individuals and yourself.

Is there any Automated Decision-making being applied to my Personal Data?

There is no automated decision-making being made using your personal data.

Will my information be shared with any third-parties?

We may share your data with the following third-parties:

1. Medical professionals e.g. ambulance service, general practitioner, locum, hospital, mental health team.

2. Care services e.g. social services, mental health services.

3. Funding services e.g. organisations that are paying or contributing to your care funding, individuals (such as relatives) who may be funding or contributing to your care funding.

4. Police – in the event of any matters involving the law.

5. Industry compliance / audit – where we are required to comply with industry requirements e.g. accreditations, auditors etc. we may need to share only data that is limited to fulfilling that purpose necessary to demonstrate compliance. This may therefore fall under the category of legitimate interest or legal obligation, depending on the nature of the audit/compliance requirement.

6. Government services – HMRC, pensions & national insurance, Care Quality Commission etc. – as required by law or order.

7. Payment processors – to enable us to process your care payments.

We use consistent third-parties who act as data processors on our behalf to provide specific services. We may share your data with them to enable us to undertake the activities as set out above. They themselves may then become data controllers once your data is shared with them. They may also introduce you to us or us to you e.g. social services, patient care teams within hospitals etc.

These providers are set out below:

Company Name / Organisation	**Activity Undertaken**	**Personal Data Shared**
Every Life Technology www.everylifetechnologies.com	Electronic care planning	Your details, medical information, complete care plan
Funding Assessors such as the local authority or the CCG	Processing your funded/part funded payments	Your *details, details of your care requirements
Pharmacy Services	Obtaining your medication	Your *details, health and prescription requirements
GP, Locum, Health Care Professional, Dentist	Ad-hoc medical requirements	Your *details and details of your condition

Company Name / Organisation	Activity Undertaken	Personal Data Shared
Social Services / Mental / Community Health Team / Other NHS Employee's	Health (Before, during or after your care)	Your *details, details of your care requirements or changing needs, concerns or issues with regards to your safety i.e. safeguarding.
NHS Trust	Referral to us	Your *details, details of your care requirements, travel requirements e.g. to meet needs of hospital visits
Your family or someone with Power of Attorney	Introduction and on-going care needs	They may provide your *details or details of your care requirements. We will only share your details or requirements with those you have authorised or requested us to OR those with the relevant power of attorney i.e. finance and/or health and welfare
Emergency Services	Protection of life or the wellbeing of others e.g. fire, medical emergency	Limited information relative to the situation. In the event of a fire we will share with the fire brigade the names, ages and conditions of those requiring evacuation. In the event of a medical emergency we will share relevant information relating to your care needs e.g. medications, conditions etc.
Accident Reporting System	We are required to record any accidents or incidents relating to those in our care	Your *details and the details of the accident or incident that occurred as well as location, date and time. This will be recorded using our unique identify system.

Company Name / Organisation	Activity Undertaken	Personal Data Shared
Misc. Providers	Religious, personal grooming, third-party activities	With your consent or at your request we will share relevant information to other parties

**'details' relates to name, address, DOB and contact information*

All the companies above either comply with our privacy policy or have appropriate security measures in place in order that they comply with the requirements under data protection and GDPR legislation.

From time to time, we may seek your consent to share information with other third-parties not included in the list above. In this instance, we will seek your explicit consent and detail what information will be shared.

What safeguards are in place to protect my personal data?

The Manor House Care Home, operates a Security By Design and By Default methodology that means we are continually checking the security, both new and current. This enables us to adhere to the Privacy by Default and By Design principles.

We will not change the use of your personal data in respect of this policy or share your data with a third party (other than those outlined above), without informing you or obtaining your consent where possible unless it is for our legitimate interest and your interests, rights and freedoms are not affected.

Retention Period

In general we will retain data for 3 years after last contact. However; due to the nature of the services we provide and our requirements to adhere to government retention guidelines these may change from time to time.

If you do not wish us to retain your data, then you have the right to be forgotten and we will at your request, destroy your data where we can legally do so and/or where we do not have a legitimate interest to retain such information e.g. any accidents that you may have had during your time with us.

If your data is required for statistical analysis, then your personal data will be anonymised to ensure that it is no longer personally identifiable.

Electronic care planning:

The Manor House Care Home uses a digital care planning system called the Pass System supplied by Everylife Technologies. This is their description of the system:
The PASSsystem is a digital care planning, monitoring and inclusion solution that has been developed by everyLIFE Technologies. It is available for care providers to purchase to manage their care business. When a care business buys The PASSsystem, they maintain all care records on the system instead of paper records.
Security
At everyLIFE, we take the security of personal information very seriously and have taken technical and organisational measures to ensure the security of the information that we hold. We are registered with the Information Commissioner's Office (ICO) and adhere to their information governance standards as demonstrated through self - assessment and submission of the IG Toolkit. All our employees have received the NHS Digital Data Security Awareness Training which meets the minimum mandatory requirement set out by the ICO. We are ISO 27001 certified / accredited, having achieved compliance for the last two consecutive years. ISO 27001 is the international standard which is recognised globally for manging the risks to the information that you hold. This includes, inter alia, having in place policies and procedures for establishing, implementing and monitoring an information security management system. In addition, we take the following measures to protect the information contained within the PASSsystem. These include:
Access control for care workers that is differentiated between that afforded to care managers
We have had an independent penetration test of our system performed by Portcullis, who are an IT Security Company part of Cisco
The database is not public facing and access is secure due to its location behind two highly protected gateways that would need to be overcome to gain access.
We take a backup, 5 times per 24hr period and store one of these in a geographically separate data centre
We have cluster infrastructure which means that if the database were to 'break', another would kick in within a matter of seconds
All customer data is stored at data centres in the UK, with a back up of this data stored separately in Ireland.

CQC accessing records and GDPR

CQC has powers under the Health and Social Care Act 2008 to access and use information where we inspectors should explain why they are asking to look at certain records. They will consider any concerns and objections raised to them, and whether they can achieve CQC's purpose by accessing the records of someone else. However, CQC relies on its legal powers to access information rather than consent, therefore may use its powers to access records even in cases where objections have been raised.

More detail on how we ensure compliance with data protection law (including GDPR) and our privacy statement is available on our website. As part of their own compliance with GDPR, providers' own privacy statements should inform people of CQC's powers to ensure their staff, people using services and their families are aware. It would be helpful for providers to include a link to CQC's privacy statement in their own.