

Privacy Notice - Residents, relatives, representatives and other contacts

This Privacy Notice explains how we comply with Data Protection Laws, including the UK General Data Protection Regulation and the Data Protection Act 2018, when collecting, using, sharing and protecting your Personal Data. “Personal Data” means any information relating to you from which you can be identified, directly or indirectly. References to ‘we’, ‘our’ or ‘us’ mean the relevant company operating a care home under the Caron Group brand or, where applicable, Caron Group Ltd. Details of the relevant care homes are available at www.carongroup.wales. In this Privacy Notice, references to ‘you’ or ‘your’ mean any resident or prospective resident, relative, representative or other resident contact whose Personal Data we collect or use.

1) How we collect your Personal Data

We may collect Personal Data about you:

- directly from you, including during enquiries, admission and review meetings, visits, telephone calls, emails, letters, complaints, surveys and other communications;
- indirectly from another person including in connection with an enquiry, admission, care arrangements, funding or other communication;
- from health and social care professionals, local authorities, health boards, commissioners, safeguarding bodies, emergency services, regulators or other organisations involved with the resident;
- from documents you provide, such as identification, evidence of authority, powers of attorney, deputyship orders, contracts or payment records;
- from our staff and records, including visitor logs, incident records and, where in use, CCTV, access-control or telephone systems; and
- from publicly available sources where this is necessary, for example to verify authority or contact details.

2) Our purposes and lawful bases

We only use your Personal Data where we have a lawful basis, and the use is necessary, reasonable and proportionate. Different bases may apply to different activities.

Contract:	Where processing is necessary to take steps at your request before entering into, or to perform, a contract with you—for example a third-party payment or top-up agreement.
Legal obligation:	Where we must comply with legal and regulatory duties, including duties relating to care services, safeguarding, complaints, record keeping, equality, health and safety, taxation, court orders and regulatory enquiries.
Legitimate interests:	Where necessary for our or your legitimate interests, or those of another person, including communicating with appropriate contacts, supporting safe and effective care, managing visits and the service, recovering sums due, investigating concerns, maintaining security and defending legal claims. Where necessary for certain purposes specified in data protection law, such as safeguarding vulnerable people, responding to emergencies and preventing or investigating crime, we may rely on the separate lawful basis of recognised legitimate interests.
Vital interests:	Where necessary to protect someone’s life, for example in a serious emergency.
Consent:	Where we ask for a genuine choice for a specific optional use. You may withdraw consent at any time, although this will not affect earlier lawful processing.

Some information may be special category Personal Data, for example information about health, disability, ethnicity, religion, sexual orientation or political opinions. Where we need to use such information, we will also rely on an additional condition permitted by law, such as health or social care, safeguarding or another substantial public interest, legal claims, vital interests or your explicit consent, depending on the purpose. Criminal offence information will only be used where authorised by law and subject to the required safeguards.

3) The Personal Data we collect about you and why

Personal Data	Why we use it
Identity and contact details, such as your name, address, email address, telephone number and preferred method or language of communication.	To identify and communicate with you and keep appropriate contact records.
Your status, for example: as a resident or prospective resident, or your relationship to a resident, and information about your role, wishes, involvement and authority, including powers of attorney, deputyship orders, advocacy arrangements and identification documents.	To verify who may act, make decisions, receive information, give instructions or enter agreements, and to respect the resident’s rights and confidentiality.
Communications and interaction records, including enquiries, emails, letters, calls, meetings, visits, requests, feedback, compliments, complaints and information you provide about yourself, the resident or others.	To respond, coordinate appropriate involvement, maintain an accurate record, manage concerns and improve our services.
Financial and contractual information, such as billing details, bank/payment information, invoices, payment history and contracts or top-up arrangements.	To administer agreements, payments, refunds, arrears and accounts and meet legal and audit requirements.

Information connected with care, incidents, accidents, safeguarding, complaints, investigations or legal proceedings where you are the resident or are otherwise involved, a witness or a relevant contact.	To provide and coordinate care, protect residents and others, investigate and respond appropriately, notify relevant bodies and establish, exercise or defend legal claims.
Health, disability, accessibility, dietary, communication or other sensitive information about you where relevant.	To assess, plan, provide and review care where you are the resident; make reasonable adjustments; support safe visits or contact; respond in an emergency; and meet legal obligations.
Visitor, security and technical information, which may include visit dates and times, signatures, vehicle details, CCTV images, access records, device or email information and recorded calls where these systems are used, and you have been informed.	To protect residents, visitors, staff and premises; manage access; investigate incidents; and maintain system and information security.

4) How long we store your Personal Data

We keep your Personal Data only for as long as it is needed for the purposes described in this notice and to meet legal, regulatory, contractual, insurance and legitimate business requirements. Retention depends on the type and context of the record. Information forming part of a resident's care, safeguarding, complaints, financial or legal record may be kept for the same period as that resident record. More temporary records, such as routine visitor or security records, are normally kept for a shorter period unless needed for an incident, complaint, investigation or legal claim. We securely delete or anonymise information when it is no longer required.

5) Who may have access to your Personal Data

Access is limited to staff who need the information for their work. Depending on the circumstances, we may share relevant Personal Data with:

- the resident, their authorised representatives and appropriate family members or contacts, subject to confidentiality, capacity and authority;
- health and social care professionals, local authorities, health boards, commissioners, advocates and other organisations involved in the resident's care, placement or funding;
- safeguarding authorities, emergency services, the police, coroners, courts, tribunals, regulators including Care Inspectorate Wales, and other public bodies where required or permitted;
- our professional advisers, auditors, insurers, banks, debt-recovery providers and legal representatives;
- contractors and service providers supporting our IT, communications, records, payment, security and other business systems, who must protect the information and act only on proper instructions; and
- another organisation in connection with a proposed or actual restructuring, transfer or sale, subject to appropriate confidentiality and data protection safeguards.

6) How we store your Personal Data and keep it safe

Your Personal Data may be held electronically and/or in hard copy. We use appropriate technical and organisational measures to protect it, including physical security, access controls, secure systems, staff training and contractual controls over service providers. Access is limited to people who need it for the purposes set out in this notice.

7) Your Data Protection rights

Depending on the circumstances and the lawful basis relied on, you may have the right to:

- be informed about how your Personal Data is used;
- request access to your Personal Data and supplementary information;
- ask us to correct inaccurate or incomplete Personal Data;
- ask us to erase your Personal Data in certain circumstances;
- ask us to restrict the use of your Personal Data in certain circumstances;
- receive certain Personal Data in a portable format where the right applies;
- object to processing based on legitimate or recognised legitimate interests, including on grounds relating to your particular situation;
- withdraw consent at any time where processing is based on consent; and
- raise a concern with the Information Commissioner's Office.

These rights are not absolute and exemptions may apply, including where information concerns another person or must be retained for legal, safeguarding or regulatory reasons. We may ask for information to verify your identity before dealing with a request.

8) How to contact us

If you have any questions about this notice or wish to exercise a Data Protection right, please contact: Data Protection Officer, First Floor, The Charter Building, Charter Place, Uxbridge UB8 1JG, or email: heretohelp@carongroup.wales. You also have the right to complain to the Information Commissioner's Office (ICO). We would welcome the opportunity to address your concern first, but you are not required to contact us before approaching the ICO. Current contact details are available at www.ico.org.uk.