Version Number	Issue Date	Revisions
V 1.0	03/2018	Initial Document by Director
V 2.0	12/11/2020	Renamed to Privacy Policy Updated to company template
V 3.0	01/09/2021	Policy reviewed and rewritten to align with RWK Policy and simplify the explanation of the data we hold, why we hold it, how we hold it, how long we retain it and how it can be accessed and by who.
V 3.1	11/01/2022	Included National Opt Out Policy and Link Included Care at Home Address
V 3.2	16/11/2022	Included section relating to collecting time sheet data and the use of photos and location data from the timesheet software
V 4	10/2023	Review by Manager
V 5.0	12/2024	Review by Manager
V6.0	06/2026	Updated to reflect the Data (Use and Access) Act 2025, ICO June 2026 complaints process requirements, UK GDPR terminology, DSAR wording, automated decision-making safeguards, processor wording and data monitoring provisions. Included retention examples.
V 6.1	10/2026	Updated to expand on automated decision making safeguards
Review Date	06/2027	By the Manager

The WCN Care Group

The WCN Care Group understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of everyone we support, employ, work with or otherwise interact with. We will only collect and use personal data in ways that are described here or in our Policies & Procedures, and in a way that is consistent with our obligations and your rights under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and any other applicable UK data protection legislation.

Fair Data Processing Notice

Within this policy we outline our Fair Data Processing Notice in line with UK GDPR, the Data Protection Act 2018 and current ICO guidance.

Information About the WCN Care Group

The WCN Care Group

Limited company registered in England under company number 11009060

Registered address: Unit 5 Callow Park, Callow Hill, Brinkworth, England, SN15 5FD

The Group Operates the following homes or services:

St Anne's Care Home
Company Name: WCN Care Ltd
Company Number: 10667607
Registered address: Unit 5 Callow Park, Callow Hill, Brinkworth, England, SN15 5FD

WCN Care at Home
Company Name: WCN Care Ltd
Company Number: 10667607
Registered address: Unit 5 Callow Park, Callow Hill, Brinkworth, England, SN15 5FD

Stour Road Care Home
Company Name: WCN Care Stour Road Care Home Ltd
Company Number: 11420743
Registered address: Unit 5 Callow Park, Callow Hill, Brinkworth, England, SN15 5FD

Chestnut Court Care Home
Company Name: Goldenpride Ltd
Company Number: 03494010
Registered address: Unit 5 Callow Park, Callow Hill, Brinkworth, England, SN15 5FD

We are regulated by the Care Quality Commission (CQC)

What Does This Privacy Notice Cover?

This Privacy Notice explains how we use your personal data: how it is collected, how it is held, and how it is processed. It also explains your rights under the law relating to your personal data.

What is Personal Data?

Personal data is defined under the UK GDPR as any information relating to an identified or identifiable living person. This means any information that can identify you directly or indirectly, including by reference to an identifier such as a name, identification number, location data, online identifier or other factors specific to you.

Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

The personal data that we use is set out below.

What Are My Rights?

Under UK data protection law, you have the following rights, which we will always work to uphold:

a) the right to be informed about our collection and use of your personal data. This Privacy Notice tells you everything you need to know, but you can always contact us if you have further queries;
b) the right to access the personal data we hold about you;
c) the right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete. This does not mean that your data can be changed to represent something untruthful at your request;
d) the right to be forgotten, that is, the right to ask us to delete or otherwise dispose of any of your personal data that we have;
e) the right to restrict (that is, prevent) the processing of your personal data;
f) the right to object to us using your personal data for a particular purpose or purposes;
g) the right to data portability. This means that if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in many cases;
h) rights relating to automated decision-making and profiling. We do not currently use your personal data to make decisions with legal or similarly significant effects solely by automated means. If this changes, we will inform you, identify the lawful basis relied upon, apply appropriate safeguards and explain your rights to request human involvement, express your views and challenge the decision.

For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in this Notice.

In some instances, if you refuse to provide us with certain information when requested, we may not be able to:

- Perform the contract we have entered into with you
- comply with our legal or regulatory obligations

Further information about your rights can also be obtained from the Information Commissioner's Office (https://ico.org.uk/) or your local Citizens Advice Bureau (https://www.citizensadvice.org.uk/).

If you have any cause for complaint about our use of your personal data, please contact us as soon as possible using the contact details in this Notice. We will handle data protection complaints in line with our internal complaints process and the requirements introduced by the Data (Use and Access) Act 2025. If you remain dissatisfied after we have responded, you have the right to lodge a complaint with the Information Commissioner's Office.

Data Protection Complaints

A data protection complaint is a complaint about how we collect, use, store, share, retain or otherwise handle personal data, or about how we respond to a request to exercise data protection rights.

Data protection complaints may be made by email, post, telephone or in person using the contact details in this Notice. Where someone complains on behalf of another person, we may need to confirm their identity and authority to act before sharing information or progressing the complaint.

Data protection complaints may also be raised through our general complaints procedure, and we will ensure they are handled in line with both that process and our data protection obligations.

We will acknowledge receipt of a data protection complaint within 30 days of receiving it. We will then take appropriate steps to investigate and respond without undue delay, including making appropriate enquiries, keeping the complainant informed where necessary and confirming the outcome of the complaint.

If the complainant is not satisfied with our response, they may refer the matter to the Information Commissioner's Office.

What Personal Data Do You Collect?

We may collect some or all of the following personal data (this may vary according to your relationship with us):

- basic personal information, including name and address, date of birth and contact details;
- financial information, including account and transactional information and history;
- information about you and your family (such as dependents, marital status, next of kin and contact details);
- information about your preferences and interests;
- visual images (such as copies of passports);
- details of any services you have received from us;
- information we receive from other sources, such as government departments and healthcare providers;
- our correspondence and communications with you.

Residents - as a care provider, we must collect some personal information on our Residents, including personal health information, which is essential to our being able to provide effective care and support. The information is contained in individual files (manual and electronic) and other record systems, all of which are subject to strict security and authorised access policies.

Employees and volunteers - we operate a recruitment policy to comply with applicable employment, safeguarding and regulatory requirements. Personal information obtained during recruitment, including CVs, application forms, references, right to work evidence, identity documents and Disclosure and Barring Service information, is securely kept, retained and disposed of in line with UK data protection law and our retention schedule.

We collect time sheet, attendance and related workforce data to manage staffing, payroll, health and safety, safeguarding, service delivery, contractual compliance and regulatory obligations. This may include staff photographs used to verify attendance and identity, and location data for staff working in the community with WCN Care at Home to confirm attendance at a client's location and

support service verification. Access to this information is limited to authorised staff and relevant service providers where necessary, and the information is retained in line with our retention schedule.

All employees are aware of their right to access any information about them.

Third parties - all personal information obtained about others associated with the delivery of the care service, including contractors and suppliers will be protected in the same way as information on Residents and employees.

Sometimes your personal data is obtained from the following third parties (depending on your relationship with us):

- Her Majesty's Revenue and Customs (HMRC), Department of Work and Pensions (DWP) and other government departments;
- National Health Service (NHS), Care & Quality Commission (CQC) and other healthcare providers;
- Clinical Commissioning Groups (CCGs) and Local Authorities (LA);
- Emergency services (police, fire and ambulance);
- Suppliers.

We may also process special category personal data for specific and limited purposes where this is necessary and lawful. Special category data may include health information, information about racial or ethnic origin, religious or philosophical beliefs, and other information requiring additional protection. We will only process this information where we have both a lawful basis under Article 6 UK GDPR and a relevant condition under Article 9 UK GDPR, such as where processing is necessary for health or social care purposes, employment obligations, safeguarding, legal obligations, substantial public interest, vital interests or where explicit consent is appropriate.

- Information about racial or ethnic origin, religious, political or philosophical beliefs;
- Physical or psychological health details or medical conditions;

How we collect information

The majority of Residents, employees and third parties personal information is collected directly from them or through form filling, mainly manually. No personal data is collected through our web-site.

With Residents, we might continue to build on the information provided through consultations and in the process of agreeing care.

With employees, personal information is obtained directly and with consent through such means as references, testimonials and criminal records checks (Disclosure and Barring Service – DBS (**https://www.gov.uk/government/organisations/ disclosure-and-barring-service**). We use a third party to complete these checks called Care Check (https://www.carecheck.co.uk).

When recruiting staff, we seek applicants' explicit consent to obtain all the information needed for us to decide to employ them.

All personal information obtained to meet our employment, safeguarding, contractual or regulatory requirements will be treated in line with UK data protection law, our confidentiality duties and our internal data protection policies. Consent will only be relied upon where it is appropriate to do so; in many cases, we may process information because it is necessary for a contract, legal obligation, legitimate interests, health and social care purposes, safeguarding or another lawful basis.

How Do You Use My Personal Data?

Under UK data protection law, we must always have a lawful basis for using personal data. This may be because the data is necessary for the performance of a contract, because we have a legal or regulatory obligation, because it is necessary for health or social care purposes, because it is in our legitimate interests, because we need to protect someone's vital interests, or because you have given consent where consent is the appropriate basis. Your personal data may be used for any of the following purposes:

- providing and managing your account;
- supplying our services to you. Your personal details are required in order for us to enter into a contract with you;
- personalising and tailoring our services for you;
- communicating with you. This may include responding to emails or calls from you;
- supplying you with information by email AND/OR post that you have opted-in to (you may unsubscribe or opt-out at any time by contacting us).

Lawful Basis for Processing Personal Data

The table below summarises the main lawful bases we rely on when processing personal data. The lawful basis may vary depending on the circumstances, the individual's relationship with us and the purpose for which the information is used.

Data subject / category	**Purpose of processing**	**Article 6 lawful basis**	**Article 9 condition, where applicable**	**Examples of data used**
Residents and people receiving care or support	Assessment, care planning, delivery of care, medication support, safeguarding, health and social care coordination, billing and service administration.	Contract, legal obligation, legitimate interests and vital interests where necessary.	Health or social care, safeguarding, substantial public interest, legal claims, vital interests or explicit consent where appropriate.	Name, contact details, care records, health information, medication records, risk assessments, financial or funding information, next of kin details and professional correspondence.
Relatives, representatives, attorneys, deputies and advocates	Communication about care, involvement in care planning, emergency contact,	Legitimate interests, legal obligation, contract and	May apply where information relates to health,	Contact details, relationship to the resident, records of communications, authority

	complaints handling, safeguarding, financial administration and confirming authority to act.	vital interests where necessary.	safeguarding, capacity, legal claims or substantial public interest.	documents, complaint records and emergency contact information.
Employees, workers, volunteers and applicants	Recruitment, employment administration, payroll, pensions, training, supervision, absence management, performance management, safeguarding, disciplinary processes, health and safety and regulatory compliance.	Contract, legal obligation, legitimate interests and consent where appropriate.	Employment, social security and social protection law, occupational health, safeguarding, substantial public interest, legal claims or explicit consent where appropriate.	Application forms, CVs, references, right to work documents, DBS information, payroll details, bank details, sickness records, training records, supervision notes, photographs, attendance records and location data where relevant.
Health and social care professionals, commissioners and external agencies	Coordinating care, referrals, reviews, safeguarding, quality monitoring, funding, contract management, regulatory reporting and continuity of care.	Legal obligation, legitimate interests, contract and vital interests where necessary.	Health or social care, safeguarding, substantial public interest, legal claims or vital interests where applicable.	Professional contact details, correspondence, care review notes, safeguarding referrals, funding information, assessment records and regulatory communications.
Suppliers, contractors and professional advisers	Contract management, procurement, payment administration, due diligence, insurance, audit, legal advice, IT support and service delivery.	Contract, legitimate interests and legal obligation.	Usually not applicable unless special category data is incidentally processed, in which case a relevant Article 9 condition will be identified.	Names, business contact details, payment details, contracts, correspondence, invoices, insurance documents and audit records.
Complainants, enquirers and people	Responding to enquiries, complaints, DSARs and other rights	Legal obligation, legitimate interests and	May apply where the complaint or request involves	Contact details, proof of identity, authority documents,

exercising data protection rights	requests, verifying identity and authority to act, investigating concerns and maintaining records of outcomes.	consent where appropriate.	health information, safeguarding, legal claims, substantial public interest or explicit consent where appropriate.	complaint details, correspondence, investigation records and outcome letters.

Where more than one lawful basis may apply, we will identify and rely on the most appropriate basis for the specific processing activity. We do not rely on consent where another lawful basis is more appropriate, and we will ensure that special category data is only processed where an Article 9 condition is met.

If a personal data breach occurs, we will assess and investigate the circumstances promptly, including the type of data involved, who may be affected, the likely risks to individuals and what action is needed to contain or reduce any impact.
Where required by law, we will report a personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of it, where feasible. Where a breach is likely to result in a risk to the rights and freedoms of affected individuals, we will inform those individuals without undue delay and provide appropriate information about the steps they can take to protect themselves.

We will keep a record of personal data breaches, including the facts relating to the breach, the effects of the breach, decisions made about reporting and the remedial action taken.

How Long Will You Keep My Personal Data?

Personal information that becomes inactive for any reason is kept securely only for as long as it is needed, before being safely disposed of.

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected. The duration for which your personal data will be kept is defined in our data retention schedule.
Examples of retention periods include care records, which are generally retained for 8 years after the end of care; staff records, which are generally retained for 6 years after employment ends; and complaints records, which are generally retained for between 3 and 6 years depending on the severity, nature and outcome of the complaint.

Where we use third-party service providers or processors, such as payroll providers, care planning systems, rostering or time and attendance systems, HR systems, DBS or recruitment checking providers, IT support, professional advisers, insurers, auditors or cloud service providers, we will take steps to ensure appropriate contractual, technical and organisational safeguards are in place. WCN Care Group remains responsible for ensuring personal data is handled safely, securely and in accordance with applicable data protection law.

How and Where Do You Store or Transfer My Personal Data?

The security of your personal data is essential to us, and to protect your data, we take a number of important measures, including the following:

- necessary technical measures to ensure personal data is protected;
- all data transferred through our systems is encrypted;
- data is not processed for any purpose other than as agreed upon in our terms and conditions;
- protect your data from loss.

Our systems are checked regularly by experts to ensure they meet all privacy standards, are protected through strong passwords and encryption and comply with our general data protection security and protection policies.

Do You Share My Personal Data?

We only share the personal information of Residents, employees and others with their consent on a "need to know" basis, whilst observing strict protocols. Most information sharing of Residents' information is with other professionals and agencies involved with their care and treatment.

Likewise, we would not disclose information about our employees without their clear agreement, for example, when providing a reference.

In some limited circumstances, we may be required legally to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

Where we provide information for statistical purposes, the information is aggregated and provided anonymously so that there is no privacy risk involved in its use.

If any of your personal data is required by a third party, as described above, we will take steps to ensure that your personal data is handled safely, securely, and in accordance with your rights, our obligations, and the third party's obligations under the law.

We will not transfer personal data outside the UK unless this is necessary and appropriate safeguards are in place. Where any supplier, system or service provider stores or accesses personal data outside the UK, we will ensure that appropriate protections are used, such as adequacy arrangements or approved contractual safeguards, and that the transfer complies with UK data protection law.

National Data Opt Out

You can opt out of data that is used for research and planning by going to the NHS website: https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/

Use of AI tools

We use Microsoft Copilot, an AI assistant within Microsoft 365, to help with administrative tasks such as drafting letters, policies and documents, and summarising information. Copilot can only access information that the person using it is already permitted to see. Information is processed by Microsoft on our behalf, is stored in the UK, and is not used to train Microsoft's AI models. AI is never used to make decisions about you, and anything it produces is checked by a person.

If you live with us: Copilot is not used for day-to-day care planning. When we review an incident, senior staff may use it to help look through the relevant care records.

If you work for us: Directors and the Executive Assistant may also use Copilot to help find information held in our systems when investigating allegations or dealing with legal matters, and to analyse staffing and payroll. This analysis looks at trends across homes and roles, not at individual performance.

Records of Copilot use are kept for 3 months and may be disclosed in response to a data protection request. Our lawful bases for this processing are the same as for the original information, as set out in this notice.

How Can I Access My Personal Data?

If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a "subject access request" or a "data subject access request" (DSAR).

All subject access requests should be made to info@wcncare.com with "ATTN: Data Protection Lead – Data Subject Access Request".

There is not normally any charge for a subject access request. If your request is manifestly unfounded or excessive, for example because it is repetitive, we may charge a reasonable fee to cover administrative costs or refuse to respond where the law permits.

We will acknowledge your DSAR as soon as reasonably practicable and will normally respond within one calendar month of receiving your request and any information needed to confirm your identity or clarify the request. Where a request is complex or you have made a number of requests, we may extend the response period by up to a further two months. If an extension is needed, we will tell you and explain why.

Before responding to a DSAR, we may need to verify your identity or, where someone is acting on your behalf, confirm their authority to act. We may also need to clarify the scope of the request. When responding, we will consider whether any exemptions apply and whether disclosure would adversely affect the rights and freedoms of another person.

How Do I Contact You?

To contact us about anything to do with your personal data and data protection, including to make a subject access request, please use the following details:
We have appointed a Data Protection Lead responsible for overseeing compliance with data protection law, supporting staff with data protection queries, monitoring our policies and procedures and acting as a point of contact for individuals and the Information Commissioner's Office where appropriate.

Email address: info@wcncare.com

St Anne' s Care Home
21-23 Wayside Road
Southbourne
BH6 3ES
01202 425642

Stour Road Care Home
14 Stour Road
Christchurch
BH23 1PS
01202 481160

WCN Care at Home
21-23 Wayside Road
Southbourne
BH6 3ES
01202 159344

Chestnut Court Care Home
9 Copse Road
New Milton
Hampshire
BH25 6ES
01425 620000

Changes to this Privacy Notice

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection. Any changes will be made available on the privacy policy page on our website.