

DATA PROTECTION — GDPR POLICY GDPR – The General Data Protection Regulations 2018 Notice for inclusion on the PH Care Group Web Site. This document is produced by and is the property of PH Care Group. We respect your privacy and will always try to protect your personal data. The purpose of this document is to inform you how we look after your personal data when you visit our website. We will also provide information about your rights and how the GDPR protects you. SECTION 1 ABOUT US AND WHAT THAT MEANS IN RELATION TO GDPR. This document aims to give you information on how we collect and process any personal data that you may have provided through your use of this website. This will include any data you may have provided if you: a. Signed up to a newsletter b. Took part in a competition c. Asked us a question about our home or services d. Anything else where you actively participated on our site This website has not been designed to attract or interact with children and we do not knowingly collect data relating to children.

Please read this document together with other information we may provide, or have provided, so that you are aware of the information that we collect and how we use that information. This document supports and is complementary to other notices and documents provided by us and is not intended to override or replace them.

The Company address for all contact and correspondence is: 17-19 Park Street, Lytham, Lancashire. THIRD PARTY LINKS OUTSIDE OF OUR CONTROL This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. PH Care Group – GDPR POLICY & PROCEDURE When you leave our website, we encourage you to read the privacy notice of every website you visit. You are responsible for your own “web presence” and the information you make available to others – please be careful what you share and who you share it with.

SECTION 2 The Personal Data we collect about you. Personal data, or personal information, means any information about an individual from which that person can be identified. You can find out more about personal data from the Information Commissioners Office. We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows: a. Identity Data - First name, last name, username, marital status, title, gender, date of birth etc. b. Contact Data – Billing address, postal address, e-mail, telephone numbers c. Aggregated Data – Statistical data, demographics etc. This form of data is not considered “personal data” as it does not directly identify you or reveal your identity. For example we may aggregate your data to calculate the percentage of users accessing a specific feature of our site, or the percentage of people accessing the site who live in Cumbria. d. Special Categories of Personal Data – We do not collect any such special category data about anyone using our site. This includes details about i. Race or ethnicity ii. Religious or philosophical

beliefs iii. Sex life or sexual orientation iv. Political opinions, trade union membership v. Health, genetics or biometrics vi. Criminal convictions or offences If you fail to provide personal data Where the law requires us to collect your personal data or, as part of a contract we have with you, and you fail to provide that data, we may not be able to carry out that contract provision. For example, where we are setting up a contract to provide you with one of our services. In such a case, we may have to cancel the service as we may not have the necessary information to carry this out safely. If this is the case, we will notify you if this at the time.

SECTION 3 HOW WE COLLECT YOUR PERSONAL DATA We may use different methods to collect data from and about you including “Direct Information Provision: a. You may give us your Name, Contact and Financial Data b. You may fill in forms or correspond with us. i. Post ii. Phone iii. E-Mail iv. Other means c. You may provide information in other ways such as: i. Applying for jobs or services ii. Create an account on our website iii. Subscribe to a newsletter or other publication iv. Request a brochure or other literature

SECTION 4 HOW WE USE YOUR PERSONAL DATA We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances: a. Performance of Contract - this means processing your data where it is necessary to carry out a contract which you have agreed to or to take steps at your request before entering into such a contract. b. Legitimate Interest - this means that it is in the interest of yours and our business to conduct and manage things to enable us to give you the best service and the most secure experience. We always consider and balance any potential impact on you (both positive and negative) and your rights before we process any personal data. We do not use your personal data where your interests are negatively impacted unless we have your consent or are otherwise required or permitted to by law. If you require further clarification on this, please contact us at the address shown above. c. Comply with a legal or regulatory obligation this means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to. **PURPOSES FOR WHICH WE MAY USE YOUR PERSONAL DATA** We have set out below a description of some of the ways in which we may use your personal data. In all cases we ensure that there is a legal basis to do so. Please note that we may process your personal data for more than one lawful reason depending on the specific purpose for which we are using your data. Please contact us at the address above for further detail and clarification. **MARKETING** We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. **PROMOTIONAL OFFERS** We may use your Identity, Contact, Usage and Profile Data to form a view of what we think you may be interested in. This is how we decide which services and offers may be relevant for you either now or in the future. You may receive marketing communications if you have requested information from us or purchased a particular service. In all cases you will only receive

information where you have opted into receiving that form of marketing. **THIRD PARTY MARKETING** We will always obtain your express opt-in consent before we share your personal data with any company outside Abbotsfield Care Home. **OPTING OUT** You can ask us or third parties to stop sending you marketing messages at any time. In most cases we have set our data collection parameters to require you to physically “opt in” to receiving information rather than requiring you to “opt out”. However, where you have purchased goods or services outside the control of Abbotsfield, you may need to follow the links and “opt out” of their system also. **COOKIES** You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please look on your web browser for how Cookies work. **CHANGE OF PURPOSE** We will only use your personal data for the purposes for which we collected it, unless we need to use it for another reason and that reason is compatible with the original purpose – or where the law requires us to do so. If you wish to get an explanation as to how the new purpose is compatible with the original purpose, please contact Abbotsfield on the address above. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

SECTION 5 WHO WE SHARE PERSONAL DATA WITH We may have to share your personal data with other people from time to time. These people will always have a legal, contractual or regulatory authority to access and see this information. These people / bodies include: a. Internal Third Parties b. External Third Parties – including i. Service Providers for IT ii. Professional Advisers such as Solicitors, Bankers, Auditors iii. Regulatory and Statutory bodies – such as CQC iv. HM Revenue & Customs v. Third parties to whom we may sell, transfer or merge parts of our business. vi. Third parties from whom we may seek to acquire part or all of their business or assets We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

SECTION 6 INTERNATIONAL TRANSFERS. If we do not transfer your data outside of the EEA (European Economic Area) we do not need to take any action. However, If we do transfer data outside the EEA, we will always ensure that the appropriate legal safeguards and mechanisms are in place to afford the highest levels of protection. It is a fact that a number of our third-party contacts (such as call centres and banks) now have bases outside the EEA. In these circumstances the enhanced robust protections are already in place.

SECTION 7 We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instruction and they are subject to a duty of confidentiality and have signed a valid confidentiality (or Non-Disclosure) agreement with us. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

SECTION 8 DATA RETENTION We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data we consider: a. The amount b. Nature and sensitivity c. The legal or regulatory requirement for personal data retention d. The potential risk of harm from unauthorised use or disclosure of personal data e. The reason we hold and process personal data f. Whether we can achieve those purposes through other means In addition, by law we have to keep some information about our customers In some circumstances you can ask us to delete your personal data. In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you. This process is usually referred to as “redacting” and is well established in law as a legitimate data sharing methodology.

SECTION 9 YOUR LEGAL RIGHTS Unless subject to an exemption under the data protection laws, you have the following rights with respect to your personal data: a. The right to request a copy of the personal data which we hold about you. b. The right to request that we correct any personal data if it is found to be inaccurate or out of date. c. The right to request your personal data is erased where it is no longer necessary to retain such data. d. The right to withdraw your consent to the processing of personal data at any time, where consent was the lawful basis for processing your data. e. The right to request that we provide you with your personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), where applicable. f. The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing. g. The right to object to our processing of personal data, where applicable. For example, where processing is based on our legitimate interests (or carrying out a task in the public interest / or official authority), or processing for scientific / historical research and statistics). You will not have to pay a fee to access your personal data (or to exercise any of your rights). However, we may charge a reasonable admin fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may even refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your data that we hold in execution of your rights. This is a security measure to ensure that personal data is not disclosed to any person who does not have the right to receive it. We may also contact you to ask you for further information in relation to your request in order to speed up our response or in order to confirm that the information request is genuine and initiated by you. We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

SECTION 10 CHANGES TO THIS GDPR NOTICE AND YOUR DUTY TO INFORM US OF CHANGES This document was last updated on the date shown as the “issue date” on this document. Please keep us informed if your personal data changes during your relationship with us. It is important that the personal data we hold about you is accurate and current.

SECTION 11 QUERIES, QUESTIONS, REQUESTS AND CONCERNS To ensure that all matters in relation to this GDPR document or any other data protection matter between you and us are managed effectively, please keep us informed of any changes or details that may be significant. If you have a complaint you should talk to us first – although there is no legal requirement for you to do this. Alternatively, you have the right to lodge a complaint with the Information Commissioners Office on 03031231113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England, UK. As in all matters which may require a legal interpretation, you are advised to seek independent legal advice on any matter relating to personal data protection, GDPR and security of personal information. The organisation is fully committed to comply with the General Data Protection Regulation (GDPR). GDPR applies to all organisations that process data relating to their employees, as well as to others including customers, contractors and clients. It sets out principles which should be followed by those who process data; it gives new and extended rights to those whose data is being processed. To this end, the organisation endorses fully and adheres to the six principles of data protection, as set out in the Article 5 of GDPR. 1. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals. 2. Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. 3. Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. 4. Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. 5. Data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. 6. Data must be processed in a

manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the organisation will:

- observe fully the conditions regarding the fair collection and use of information including the giving of consent
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (ie the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- take appropriate technical and organisational security measures to safeguard personal information
- publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection
- ensure that personal information is not transferred abroad without suitable safeguards.

DATA SECURITY All staff are responsible for ensuring that:

- any personal data that they hold is kept securely
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe. paper forms where necessary for temporary record keeping.