Winash Residential Care Home

OP 08 – Winash Privacy Notice

Reference No:	OP 08	**Version No:**	Two		

Policy Documents to read alongside this Policy	All other Policies and Procedures

Classification of Document: **Corporate**

Area for Circulation: **Internal use for Winash Ltd staff**

Authors: Mr Kurt Saunders **MSc PGCE Grad IOSH OSHCR MIHM SFIIRSM FRSPH FCMI**

Registered Occupational Safety & Health Consultant
HR Management Consultant CIPD Registered

Ms Claire Cook at Winash Ltd

Executive Lead: **Heather House Director**

Group Consulted/Via Committee:

Ratified by: **Heather House Director**

Date Published: **October 1st 2018**

Version Number	Date of Review	Reviewer Name	Completed Action	Approved By	Date Approved	New Review Date
Two	17/08/2020	Claire Cook	Adding NHS opt-out statement	Heather House	17/08/20	March 2021

Winash Employee & Service User privacy notice

Winash is aware of its obligations under the General Data Protection Regulation (GDPR) and is committed to processing your data securely and transparently. This privacy notice sets out, in line with GDPR, the types of data that we hold on you as an employee or Service User of the Company. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

This notice applies to current and former employees, workers, contractors and Service Users and Service Users relatives.

1. Data controller details

Winash is a data controller, meaning that it determines the processes to be used when using your personal data. Our contact details are as follows:

Winash Rest Home ("Winash"): A company limited by guarantee in England under number 5953260.

Registered Office: 7 – 9 Albert Road, Clevedon, North Somerset, BS21 7R. Telephone

01275 873 129. Email info@winash.co.uk

2. Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment or residency and in ways that have been explained to you
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed

3. Types of data we process

We hold many types of data about you, these may include:

- your personal details including your name, address and previous addresses, date of birth, email address, phone numbers
- your photograph, gender and marital status

dependants, next of kin and their contact numbers, medical or health information including whether or not you have a disability

- information used for equal opportunities monitoring about your sexual orientation, religion or belief and ethnic origin
- information included on your CV including references, education history and employment history
- documentation relating to your right to work in the UK
- driving licence, bank details, tax codes, National Insurance number
- current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to your employment with us
- letters of concern, formal warnings and other documentation with regard to any disciplinary proceedings
- internal performance information including measurements against targets, formal warnings and related documentation with regard to capability procedures, appraisal forms
- leave records including annual leave, family leave, sickness absence etc
- details of your criminal record, your DBS check number and training details
- CCTV footage, call recordings and building entry card records.

4. How we collect and store your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise or initial assessment where we will collect the data from you directly. This includes the information you would normally include in a CV or a recruitment cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as your doctor, 3rd party health or social care professionals, discharging hospital, your Local Authority, your Next of Kin, employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in personnel files, Service User files and care plan folders or within Winash's HR or IT systems. Some information is stored on 3rd party IT systems who have their own Privacy Policy.

5. Why we process your data

The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment /service user contract that we are party to • in order to carry out legally required duties

  in order for us to carry out our legitimate interests to protect your interests and
- where something is done in the public interest.

All of the processing carried out by us falls into one of the permitted reasons.

Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data in order to:

- carry out the employment contract that we have entered into with you and ensure you are paid.
- Provide appropriate care and medication

We also need to collect your data to ensure we are complying with legal requirements such as:

- ensuring tax and National Insurance is paid
- carrying out checks in relation to your right to work in the UK and making reasonable adjustments for disabled employees and service users.
- CQC registration compliance

We also collect data so that we can carry out activities which are in the legitimate interests of the Company. We have set these out below:

- making decisions about who to offer initial employment to, and subsequent internal appointments, promotions etc
- providing appropriate care and support
- making decisions about whether we can meet your care needs
- making decisions about salary and other benefits
- providing contractual benefits to you
- maintaining comprehensive up to date personnel/service users records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises
- offering a method of recourse for you against decisions made about you via a grievance procedure
- assessing training needs

- implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments
- gaining expert medical opinion when making decisions about your fitness for work
- managing statutory leave and pay systems such as maternity leave and pay etc
- business planning and restructuring exercises
- dealing with legal claims made against us

  preventing fraud ensuring our administrative and IT systems are secure and robust against unauthorised access
- Obtaining medical history for service users to enable a detailed care plan to be implemented, based on the assessed needs of the service user.

6. <u>Special categories of data</u>

Special categories of data are data relating to your health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, trade union membership genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations • we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data:

- for the purposes of equal opportunities monitoring
- in our sickness absence management procedures
- to determine reasonable adjustments
- to determine the appropriate care needs of each service user

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

7. Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, but, may also be collected during your employment. We use criminal conviction data to assess your suitability for employment. We process this data because of our legal obligation and to adhere to CQC regulation.

8. If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your employment/service user contract. If you do not provide us with the data needed to do this, we will unable to perform those duties e.g. ensuring you are paid correctly or administering the correct medication. We may also be prevented from confirming, or continuing with, your employment with us in relation to our legal obligations if you do not provide us with this information eg confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records check.

9. Sharing your data

Your data will be shared with staff/colleagues within the Company where it is necessary for them to undertake their duties. This includes, for example, the HR department for maintaining personnel records and kitchen staff to enable them to provide appropriate meals.

We share your data with third parties in order to:

- obtain references and DBS checks as part of the recruitment process
- comply with legal obligations to Government bodies ie. HMRC and DWP
- obtain medical records and assess care needs
- provide the correct medication

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us.

We do not use or share your data for research purposes or for planning improvements to health and care services as per the NHS Opt-out Policy. All residents have a choice to opt-out of having their personal information used by healthcare services that do use patient information for research and planning. Patients can view or change their national **data opt-out** choice at any time by using the online service at www.**nhs**.uk/your-**nhs-data**-matters or by calling 0300 3035678.

We will not share your data with bodies outside of the European Economic Area unless you explicitly request us to do so, in writing. Where we may store your data outside of the European Economic Area. We only use companies who store the data in a way than complies with EU and UK data protection laws.

10. Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against

such, ie. Keeping an up to date data audit, enabling 2 step authentication and regularly reviewing our confidentiality policy.

Where we share your data with third parties, we have obtained copies of their privacy statements to ascertain whether your data is held securely and in line with GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

11. How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for, which will be at least for the duration of your residency/employment with us though in some cases we will keep your data for a period of 6 years after your residency/employment has ended. Retention periods can vary depending on why we need your data, as set out below:

Medication and care records: 6 years from the end of service users contract

Application and Recruitment Records: 6-12 months

Pension Benefits: 12 years from the ending of any benefit payable

All Personnel Files and Training Records: 6 years from the end of employment

Redundancy & sickness Records: 6 years after employment ends

12. Automated decision making

No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement).

13. Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request. You can read more about this in our GDPR policy which is available on request
- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe

there is no reason for us to continue processing it (providing, where deleting it will not mean we are in breach of any legal obligations)

- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct
- the right to portability. You may transfer the data that we hold on you for your own purposes
- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

14. Data Protection Officer

If you wish to exercise any of the rights explained above, please contact the Company's Data Protection Officer:

Heather House, Director, Winash Ltd, 9 Albert Road, Clevedon, North Somerset, BS21 7RP. Tel. 01275 873 129. Email. heather@winash.co.uk

Data security

The Company adopts procedures designed to maintain the security of data when it is stored and transported.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees and service users should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by Ms Heather House. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the **Company's disciplinary procedure**. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Company becoming aware of it and may be reported in more than one instalment. **www.ico.org.uk Tel: 0303 1231113**

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the Company will do so without undue delay.

Training

New and existing employees must read and understand the policies on data protection as part of their induction and CPD training.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company, Ms Heather House, are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.