GDPR

(GENERAL DATA PROTECTION REGULATIONS)

VERSION No	2
REVIEWED BY	Registered Manager (MP)
NUMBER OF PAGES	28

INDEX

Policy Statement

On the 25th May 2018 the new Data Protection Act 2018, which is based on the General Data Protection Regulations (GDPR) replaces the Data Protection Act 1998 in its entirety. It replaces the existing Data Protection Laws to make them fit for the digital age in which ever increasing personal data is being processed. The Act sets new standards for protecting personal data. Gives people more control over the use of their data and assists in the preparation for a future outside of the EU. There are 4 main matters provided for in the Regulations and these are:

- General Data Processing
- Law Enforcement Data processing
- Data Processing for National Security Purposes
- Enforcement

All of the above need to be set in the context of international, national and local data processing systems which are increasingly dependent upon internet usage for exchange and transit of data. The UK must lock into international data protection arrangements, systems and processes and this Act updates and reinforces the mechanism to enable this to take place.

We may have to collect and use information about people. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out activities. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

Overview of the GDPR Act

The Act is structured in 7 parts, each of which covers specific areas. These are:

Part 1: Preliminary: This sets out the parameters of the Act, gives an overview, explains that most processing of personal data is subject to the Act and gives the terms relating to the processing of personal data.

Part 2: General Processing: This supplements the GDPR and sets out a broadly equivalent regime to certain types of processing to which the GDPR does not apply.

Part 3: Law Enforcement Processing: This covers;

- "competent authority"
- meaning of "controller" and "processor"
- data protection principles
- safeguards in regard to archiving and sensitive processing
- rights and access of the data subject, including erasure
- implements the law enforcement directive
- controller and processor duties and obligations
- records
- co-operation with the ICO commissioner
- personal data breaches
- the remedy of such breaches
- position of the data protection officer and their tasks
- transfer of data internationally to particular recipients
- national security considerations
- special processing restrictions and reporting of infringements.

Part 4: Intelligence Services Processing: This covers only data handled by the above e.g. MI5 and MI6 and includes rights of access, automated decisions, rectification and erasure, obligations relating to security and data breaches.

Part 5: The Information Commissioner: This covers

- general functions including publication of Codes of Practice and guidance
- their International role
- their responsibilities in relation to specific Codes of Practice
- consensual audits
- information to be provided to the Commissioner
- confidentiality and privileged communication
- fees for services
- charges payable to the commission
- publications
- Notices from the Commissioner
- reporting to parliament.

Part 6: Enforcement: This covers the new enforcement regime in relation to all forms of Notice issued by the Commissioner

- powers of entry and inspection
- penalty amounts
- appeals
- complaints
- remedies in the court
- offences
- special purpose proceedings.

Part 7: Supplementary and Final Provision: This covers legal changes which the new Act alters in relation to other legal matters, e.g. Tribunal Procedure rules, definitions, changes to the Data Protection Convention etc. and List of Schedule(s).

GDPR is a huge piece of legislation, the majority of which is outside the remit of service providers working within the Adult Health and Social Care Sector. The I.C.O. (Information Commissioner's Office) confirms that many concepts and principles are much the same and businesses already complying with the current law are likely to be already meeting many of the key requirements of the GDPR and the new Act.

The Information Commissioner says the new Act represents a "step change" from previous laws. "It means a change of culture of the organisation. That is not an easy thing to do, and its certainly true that accountability cannot be bolted on: it needs to be a part of the organisations overall systems approach to how it manages and processes personal data". It's a change of mindset in regard to data handling, collection and retention.

We need to stop taking personal data for granted, its not a commodity we own: its only ever on loan. Individuals have been given control and we have been given fiduciary duty of care over it!

As an organisation handling personal data on a day to day basis, this policy sets out the requirements of the new Act and how we, as an organisation will meet our legal obligations. Staff awareness and understanding of their responsibilities in regard to the handling, collection and retention of data will be core to the successful embedding of this policy.

Preparation: (The 12 Steps)

In order to comply with the requirements of the Act preparation should include the completion of the 12 steps

- **Awareness**
- **Information we hold**
- **Communicating privacy information**
- **Individuals rights**

- **Subject access requests**
- **Lawful bases for processing**
- **Consent**
- **Children**
- **Data Breaches**
- **Data Protection by Design and Data Protection Impact Assessments**
- **Data Protection Officers**
- **International Data**

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now.
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

The ICO has issued this guidance as the start of the preparation. They have also made clear that they are aware that for small companies in particular time can be a factor in this preparation, but it is important to start the 12 steps in order to show compliance. As an organisation we are preparing for this new Act by completing these 12 steps.

Definitions

The GDPR applies to "Controllers", "Processors" and "Data Protection Officer" and to certain types of information, specifically, "Personal Data" and "Sensitive Personal Data" referred to in the Act as Special Categories of Personal Data".

a) **"Controllers":** This role determines, on behalf of the organisation, the purposes and means of processing personal data.
b) **"Processors":** This role is responsible for processing personal data on behalf of a controller. The Act places specific legal obligations and requirements to keep and maintain records of personal data and processing activities. This role has legal liabilities if responsible for any breach.
c) **Data Protection Officer:** This role is a must only in certain circumstances if you are:
    i) A public authority (except for courts)
    ii) Carry out large scale systematic monitoring of individuals e.g. online behaviour tracking, or
    iii) Carry out large scale processing of special categories of data, or data relating to criminal convictions and offences e.g. Police, DBS Bodies, Prison Service etc.
d) **"Personal Data":** This means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. So, this would include name, reference or identification number, location data or online identifier. This reflects changes in technology which incorporates a wide range of different identifiers. Personal Data applies to both automated and manual filing systems. It can also apply to pseudonymised e.g. key-coded can fall within the GDPR dependent on how difficult it is to attribute the pseudonym to a particular individual. Race, ethnic origin, politics, religion, trade union membership, sex life or sexual orientation.
e) **"Special Categories of personal Data":** This category of data is more sensitive and much more protected. Sensitive personal data specifically includes genetic data, biometric data, health, race, ethnic origin, politics, religion, trade union membership, sexual orientation Safeguards apply to other type of data e.g. criminal convictions and offences; intelligence data etc.
f) **"Criminal offence data":** is data which relates to an individual's criminal convictions and offences.
g) **"Data processing":** is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection Principles

The GDPR sets out the following principles for which organisations are responsible and must meet. These require that personal data shall be:

a) **Processed lawfully, fairly and in a transparent manner in relation to individuals;**
b) **Be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with purposes, further processing for archiving purposes in the**

public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.**

d) **Accurate and where necessary, kept up to date, every reasonable step must be taken that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;**

e) **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer purposes in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the appropriate technical and organisational measures required by the GDPR (the safeguards) in order to safeguard the rights and freedoms of individuals; and**

f) **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.**

g) **"The controller shall be responsible for, and be able to demonstrate, compliance with the principles" Article 5 (2) GDPR**

"Lawful bases" for processing: There are 6 lawful bases for processing data. These are:

- **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked us to take specific steps before entering into a contract.
- **Legal Obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
- **Vital Interests:** the processing is necessary to protect someone's life.
- **Public Task:** the processing is necessary for us to perform a task in the public interest, or for official functions and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (Does not apply if a public authority is processing data to perform its official tasks).

i) **Consent:** The GDPR sets a high standard here. Consent means offering individuals real choice and control. Consent practices and existing paperwork will need to be refreshed and meet specific requirements. These are:

- ⚠ Positive opt-in, no pre-ticked boxes or other method of "default" consent
- ⚠ A clear and specific statement of consent
- ⚠ Vague or blanket consent is not enough
- ⚠ Keep consent requests separate from other terms and conditions
- ⚠ Keep evidence of consent – who, when, how, and what you told people
- ⚠ Keep consent under review
- ⚠ Avoid making consent to processing pre-condition to any service
- ⚠ Employers need to take extra care to evidence that consent is freely given, and should avoid over reliance on consent

Consent is one lawful basis to consider but organisations in a position of power over individuals should consider alternative "lawful bases". If we would still process their personal data without consent, then asking for consent is misleading and inherently unfair.

PLEASE NOTE
Consent within this policy relates only to data processing not Health or Support in a Social Care context. You must still use consent as defined within the Mental Capacity Act 2005 to deliver services

ii) **Legal Obligation:** Put simply, the processing is necessary for us as an organisation to comply with the law, e.g. the Health and Social Care Act 2008 (Regulations 2014), which requires us

as providers to collect, handle and process data in a prescribed manner.

iii) Legitimate Interests:

- This is the most flexible lawful basis for processing
- It is likely to be appropriate where we process in ways that people would reasonably expect us to, with a minimal privacy impact, or where there is a compelling justification for the processing
- There are 3 elements to consider when using this lawful base. We need to:
  - i) Identify a legitimate interest
  - i) Show that the processing is necessary to achieve it: and balance it against the individual's interests, rights and freedoms
  - ii) Legitimate interests can mean ours, interest of third parties, commercial interests, individual or social benefits
- The processing must be necessary
- A balance must be struck between our interests, the individual's and would it be reasonable to expect the processing, or would it cause unnecessary harm, then their interests are likely to override our legitimate interests
- Keep a record of your legitimate interest's assessment (LIA) to help you demonstrate compliance

The above are the 3 most pertinent bases for Health and Social Care data processing activity. ***Contract, Vital Interests or Public Task*** *apply within specific work settings and would be difficult to meet because service providers are subject to specific legislative and regulatory requirements in order to work within a "Regulated Activity".*

"Lawful bases" *must be determined by the organisation before processing of any personal data and it is vital that thorough consideration is given to this decision. Service users or residents must be aware of the lawful base used by this organisation to process their personal data*

Individual Rights: The GDPR provides the following rights for individuals:

a) Right to be informed
b) Right of access
c) Right to rectification
d) Right to erasure
e) Right to restrict processing
f) Right to data portability
g) Right to object
h) Rights in relation to automated decision making and profiling

All relevant guidance to individual rights is not yet complete, Working Party (WP)29 will continue to work and produce such guidance as is thought appropriate.

Any individual request which falls into the above categories this organisation will follow the relevant guidance currently available on the following website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/

Types of Data Held for Employees

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the some within our computer systems. The data is processes mainly due to:

- Legal obligations: such as DBS checks, NI as HMRC required collection of contribution;
- Contractual: such as Bank accounts to transfer wages payments;
- Legitimate interests: such as qualifications (though this may be considered as Legal obligation under the Health and Social Care Act) or a photograph of staff member for ID purposes

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on education and employment history etc

c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to employment with us, including:
    i) job title and job descriptions
    ii) salary
    iii) wider terms and conditions of employment
    iv) details of formal and informal proceedings involving staff member such as letters of concern, disciplinary and grievance proceedings, annual leave records, appraisal and performance information
    v) internal and external training modules undertaken
    vi) photograph
    vii) criminal records and DBS

All of the above information is required for our processing activities.

Privacy notices, transparency and control

A privacy notice must have as a minimum:

- ⚠ **who you are**
- ⚠ **what you are going to do with their information**
- ⚠ **who it will be shared with.**

Being transparent, and providing accessible information, is core to compliance and the GDPR. Privacy notices is the most common way to meet the GDPR requirements.

Transparency, in a governance or business context, is honesty and openness and the more transparent we can be the more easily understood and accessible our services become to the people who use them. In the context of data processing is simply that: **"it should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of their personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processor and further information to ensure fair and transparent processing in respect of the confirmation and communication of personal data concerning them which is being processed."**

ICO (Information Commissioner's Office): Role and Function.

With regard to the changes within the new GDPR, National Supervising Authorities in all EU member states have had their powers of enforcement enhanced. Our I.C.O. in the UK's supervising authority. Within the Enforcement Toolbox, the Information Commissioners Office known as the I.C.O., can now issue substantial fines of up to 20 million, or, 4% of an organisation's global turnover for certain data protection infringements. Fines, when appropriate, will be of the discretion of the I.C.O. with considerable variations expected to be levied. There are no fixed penalties or minimum fines, though there are different maximum fines for different breaches. The GDPR also empowers the I.C.O. to create tailor made solutions to deal with infringements brought to their attention. This does not mean that organisations can relax about compliance, but diligent small and medium sized organisations can take comfort in the fact that they are unlikely to face the sort of punitive fines that rogue tech giants could in order to bring them to head.

Remember: the highest imposed fine limit was £500,000 under the old Act (1998) but the highest fine ever imposed was £400,000 to TalkTalk for failings in connection with a cyber-attack in 2016. The Information Commissioner herself is playing down the "scaremongering because of misconceptions". £20 million fines could put businesses out of business and that is not the intention of the GDPR, though there is a seismic shift in the number of fines that could be imposed.

The role and scope of the I.C.O. has not fundamentally changed, but rather has been expanded and enhanced via the new GDPR.

Codes of Conduct and Certification Mechanisms.
Although the use of any of the above is encouraged by the GDPR it is not obligatory. If an approved code of conduct or certification scheme becomes available that covers our processing activity, consideration will be given to working towards such a scheme as a way of demonstrating our compliance. The I.C.O. will develop its own code of conduct as it has already worked with the Direct Marketing Commissions Code of Conduct: DMA Code.

Codes of Practice.
The Act enhances the role of the Information Commission's Office (I.C.O.) in the compilation of such Codes and these will be available in due course. It is important that we are regularly checking the I.C.O. website in order to keep up with current guidance.

Derogations and Exceptions
The Act provides that member states of the EU can provide their own national rules in respect of specific processing activities.

All Data Controllers must be familiar with Schedules 1-18 of the GDPR as these are the lawful exemptions pertinent to many other legal frameworks and Acts. These Schedules cover things such as Parliamentary Privilege, Health and Social Work, Criminal Convictions (Additional Safeguards), Research, Statistics and Archiving, Education Child Abuse, and include specific provisions for data processing within the Schedule(s).

***For example:** Schedule 15: Powers of Entry and Inspection. This Schedule sets out clearly the powers of the Information Commissioner's Office in relation to warrant(s) issued by the courts which allow the I.C.O. to enter premises and inspect data field there, including the seizure of documents. Schedule 18 is where all the legislative changes, in all pertinent primary legislation is found, including the repeal of the Data Protection Act 1998. As the Act is embedded in to the organisation, Data controllers, their role and responsibilities, will need to be reviewed and revised to ensure compliance.*

The GDPR Policy

This organisation believes that all data, required for the delivery of the service and the lawful running of the organisation must be collected, handled, maintained and stored in accordance to the requirements of the Data Protection Act.

The General Data Protection Regulations (GDPR) form the basis of the Act but in order to be effective and compliant with its requirements, the Related Policy list should be viewed as core to this policy, as should Section 1 and the Related Guidance links.

***PLEASE NOTE:** All Guidance from the ICO should be considered "Live Documentation" and regularly checked until all Codes of Practice and Guidance are issued. Working Party 29 known as WP29 is a representative body from each of the EU member states who have developed and worked on the Act. WP29 still sits and meets in the European Parliament until all of the complexities of the Act have been clarified and amended into law.*

Lawful Bases
We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the employee's consent in order to process data. The manager is undertaking a records audit to determine the lawful basis for records kept and processed, to determine required actions.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

Data Protection Principles

The Act sets out 8 Principles which must be adhered to when processing data *(Please refer to the Related Guidance links for further information).* The GDPR sets out the following principles for which this organisation is responsible and must meet. These require that personal data shall be:

a) **Processed lawfully, fairly and in a transparent manner in relation to individuals;**
b) **Be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with purposes,** *further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes;*
c) **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.**
d) **Accurate and where necessary, kept up to date, every reasonable step must be taken that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;**
e) **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;** *personal data may be stored for longer purposes in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the appropriate technical and organisational measures required by the GDPR (the safeguards) in order to safeguard the rights and freedoms of individuals;* **and**
f) **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.**
g) **Compliant with the relevant GDPR procedures for international transferring of personal data**
h) **"The controller shall be responsible for, and be able to demonstrate, compliance with the principles" Article 5 (2) GDPR**

This company is not required to have a 'Data Controller', however, the manager is responsible for the compliance with the GDPR

Individual Rights

There are several changes here in particular the Right of Access in relation to timescales and fees. These must be fully understood in relation to anyone submitting a Subject Access request. Please refer to the related Guidance Link. The GDPR provides the following rights for individuals:

- ***Right to be informed***
- ***Right of access***
- ***Right to rectification***
- ***Right to erasure***
- ***Right to restrict processing***
- ***Right to data portability***
- ***Right to object***
- ***Rights in relation to automated decision making and profiling***

Each of the above rights has its own Best Practice Process which you will find here:
https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Privacy Notices

This is a new requirement for data processing, it is an accessible information declaration which should set out clearly how we will gather, use handle, store and process personal data.

The Code uses the term "Privacy Notice" to describe all the privacy information that you make available or provide to individuals when you collect information about them. It is often argued that people's expectations able personal data are changing, particularly through the use of social media, the use of mobile apps and the willingness of the public to share personal information via these platforms. However, as an organisation we are increasingly aware of the fragile trust which can be easily broken through data breaches and are therefore seeking transparency as a means of building trust and confidence with users of our services. It is the spirit of the Act that privacy, transparency and control

become a given for users.

Being transparent by providing a privacy notice is an important part of fair processing. When planning a privacy notice, we need to consider the following:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

The Privacy notice must be easily understood by the people intended for and include all of the above, and all relevant privacy notices will made available to the relevant people, as well as on our website, staff policies and procedures, residents' handbook and the TV monitors around the home.

Privacy and Electronic Communications Regulations (PECR)
This guide issued by the ICO covers specifically electronic marketing messages i.e. phone, fax, email or text, and includes the use of cookies. It introduces specific roles on the above keeping such communication services secure and user's privacy in regard to traffic and location data, itemised billing, line identification and directory listings

The Data Protection Act 2018 still applies if you are processing personal data. The PECR sets out some extra rules for electronic communications and please be mindful of electronic schedule systems which will also come under PECR

File Retention
The GDPR sets out Guidance on files and retention including archiving, specifically Health and Social Care personal data is generally exempt.

As a provider of services, file and retention guidelines are in place from our Regulator which includes CQC and the NHS as well as Local Authorities via the Service Specification within any contractual arrangements. A periodic check of the Regulator's Guidance is a part of the review of this policy

Compliance
In order to meet the requirements of the Act a thorough knowledge of the Guidance should be the priority for the Data Controller / person responsible.

It is also important that the Act is placed in the context of other compliance requirements namely The Health and Social Care Act 2008 (Regulated Activities) (Regulations 2014) and all other lawful requirements such as Regulation 18 Staffing to name but one.

In recognition of the complexities of the Act, the ICO has set up an advice service for small organisations. https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/

Access to Data
As stated earlier, people: employees and service users and where appropriate their representatives, have a right to access the personal data that we hold on them. To exercise this right, employees should make a Subject Access Request, residents have the right to access their records under the Health and Social Care Act. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit if necessary.

No charge will be made for complying with a request *unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.*

Further information on making a subject access request is contained in our Subject Access Request section later.

Data Disclosures
The Company may be required to disclose certain data / information to any person. The circumstances leading to such disclosures include:

a) A person's benefits operated by third parties;
b) disabled individuals - whether any reasonable adjustments are required to assist them;
c) individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
d) for Statutory Sick Pay purposes;
e) HR management and administration - to consider how an individual's health affects his or her ability to do their job;
f) the smooth operation of any employee insurance policies or pension plans;
g) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.
h) Inspections by relevant regulatory organisations such as CQC (Care Quality Commission)
i) In an emergency such as Ambulance Paramedics, GP, etc.
j) For residents: under the Health and Social Care Act, to share information and health and care records with other professionals such as GP, Social worker, opticians, etc. for the benefit of the resident's health and wellbeing.

The above list is not exhaustive. These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security
All our employees are aware that hard copy personal information should be kept safe in a locked office.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. *No files or written information of a confidential nature are to be left where they can be read by unauthorised people.*

Where data is computerised, it is 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 is kept safe in a locked office.

Employees must 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.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it is protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using password protection: a folder should be created to store the files that need extra protection ensuring that laptops or USB drives are not left 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.

Third Party Processing
Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

International Data Transfers
The Company does not transfer personal data to any recipients outside of the EEA. Data is stored on a 'cloud', safely and password protected. When necessary a limited access to a third party is authorised.

Requirement to Notify Breaches
All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification section.

Training Statement
All staff must be made aware of the changes to the Data Protection Legislation during their Induction. All relevant identified posts, more specifically, the admin assistant and qualified nursing staff who are involved in the processing of data, must have specific training on the requirements that are now place on organisations. The Data Controller should be responsible for the cascading of any training.

People's Rights in Relation to their Data

a) **Aim:** This policy outlines the rights that data subjects (people) have, under the General Data Protection Regulation (GDPR), in relation to the data about them that we hold. *Data subjects, for the purposes of this policy, includes employees, residents / clients (current, prospective and former) and contractors.*

b) **The Right to be Informed:** In order to keep data subjects informed about how we use their data, we have a privacy notice for employees, residents, applicants and contractors. Relevant Privacy notices are made available to the appropriate persons. *Our privacy notices set out:*

i. the types of data we hold and the reason for processing the data;
ii. our legitimate interest for processing it;
iii. details of who the data is disclosed to and why.
iv. how long we keep the data for, or how we determine how long to keep the data for (usually prescribed by legislation);
v. where the data comes from;
vi. the rights as a data subject;
vii. the absolute right to withdraw consent for processing data where consent has been provided and no other lawful reason for processing the data applies;
viii. the right to make a complaint to the Information Commissioner if and when felt that rights have been breached;
ix. whether we use automated decision making and if so, how the decisions are made, what this means for the data subject and what could happen as a result of the process;
x. the name and contact details of the person responsible for data compliance.

c) **The Right of Access:** Data subjects have the right to access their personal data which is held by us. More details on how to request access to the data by reading our Subject Access Request section.

d) **The Right To 'Correction':** If people discover that the data we hold about them is incorrect or incomplete, they have the right to have the data corrected.

Usually, we will comply with a request to rectify data within one month unless the request is particularly complex in which case we may write to you to inform you we require an extension to the normal timescale. The maximum extension period is two months.

The person requesting the correction will be informed if we decide not to take any action as a result of the request. In these circumstances, the person may to complain to the Information Commissioner and have access to a judicial remedy.

Third parties to whom the data was disclosed will be informed of the rectification.

e) The Right of 'Erasure': In certain circumstances, we are required to delete the data we hold. Those circumstances are:

i. where it is no longer necessary for us to keep the data;
ii. where we relied on a person's consent to process the data and that person subsequently withdraw that consent. Where this happens, we will consider whether another legal basis applies to our continued use of your data;

iii. where a person objects to the processing (see below) and the Company has no overriding legitimate interest to continue the processing;
iv. where we have unlawfully processed personal data;
v. where we are required by law to erase the data.

If a person wishes to make a request for data deletion: we will consider each request individually, however, you the person should be aware that processing may continue under one of the permissible reasons. Where this happens, the person will be informed of the continued use of their data and the reason for this.

Third parties to whom the data was disclosed will be informed of the erasure where possible unless to do so will cause a disproportionate effect on us.

f) **The Right of 'Restriction':** data subjects have the right to restrict the processing of their data in certain circumstances. We will be required to restrict the processing of a personal data in the following circumstances:
i. where the data subject tells us that the data we hold on you is not accurate. Where this is the case, we will stop processing the data until we have taken steps to ensure that the data is accurate;
ii. where the data is processed for the performance of a public interest task or because of our legitimate interests and a person have objected to the processing of data. In these circumstances, the processing may be restricted whilst we consider whether our legitimate interests mean it is appropriate to continue to process it;
iii. when the data has been processed unlawfully;
iv. where we no longer need to process the data but a data subject needs the data in relation to a legal claim.

If a person wish to make a request for data restriction: where data processing is restricted, we will continue to hold the data but will not process it unless the data subject consents to the processing or processing is required in relation to a legal claim.

Where the data to be restricted has been shared with third parties, we will inform those third parties of the restriction where possible unless to do so will cause a disproportionate effect on us.

The data subject will be informed before any restriction is lifted.

g) **The Right to Data 'Portability':** People have the right to obtain the data that we process on them and transfer it to another party. Where our technology permits, we will transfer the data directly to the other party. Data which may be transferred is data which:
i. the data subject has provided to us; and
ii. is processed because the person has provided their consent or because it is needed to perform the employment contract between us; and
iii. is processed by automated means.

If a person (a staff member or a resident) wishes to exercise this right, please speak to the manager.

We will respond to a portability request without undue delay, and within one month at the latest unless the request is complex or we receive a number of requests in which case we may write to the person to inform them that we require an extension and reasons for this. The maximum extension period is two months. We will not charge for access to data for this purpose.

The person requesting the data transfer will be informed if we decide not to take any action as a result of the request, for example, because the data they wish to transfer does not meet the above criteria. In these circumstances, the person can complain to the Information Commissioner and have access to a judicial remedy.

The right to data portability relates only to data defined as above. Data subjects should be aware that this differs from the data which is accessible via a Subject Access Request.

h) **The Right to 'Object':** people have a right to require us to stop processing their data; this is known as data objection. Data subjects may object to processing where it is carried out:

i. in relation to the Company's legitimate interests;
ii. for the performance of a task in the public interest;
iii. in the exercise of official authority; or
iv. for profiling purposes.

If a person wishes to object, the person should inform the manager. In some circumstances we will continue to process the data the person has objected to. This may occur when:

- we can demonstrate compelling legitimate reasons for the processing which are believed to be more important than the person's rights; or
- the processing is required in relation to legal claims made by, or against, us.

If the response to the person's request is that we will take no action, the person will be informed of the reasons.

i) **Right Not to Have Automated Decisions Made About Data Subjects:** *Data subjects have the right not to have decisions made about them solely on the basis of automated decision-making processes where there is no human intervention, where such decisions will have a significant effect on them.* ***However, the Company does not make any decisions based on such processes.***

However, we may carry out automated decision making with no human intervention in the following circumstances:

- when it is needed for entering into or the carrying out of a contract with the data subject;
- when the process is permitted by law;
- when the person has given explicit consent.
- In circumstances where we use special category data, for example, data about a person's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, the Company will ensure that one of the following applies to the processing:
  - you have given your explicit consent to the processing; or
  - the processing is necessary for reasons of substantial public interest.

Data Subject Access Request

a) **Aim:** People have a right, under the General Data Protection Regulation, to access the personal data we hold on them. To do so, a data subject should make a subject access request, and this sets out how a person should make a request, and our actions upon receiving the request.

b) **Definitions:**

- **"Personal data" is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including their name.**
- **"Special categories of personal data**" includes information relating to:
  - *race*
  - *ethnic origin*
  - *politics*
  - *religion*
  - *genetics*
  - *biometrics (where used for ID purposes)*
  - *health*
  - *sex life or*
  - *sexual orientation*

c) **Making a Request:** Although subject access requests may be made verbally, we would advise that a request may be dealt with more efficiently and effectively if it is made in writing.

Requests made in relation to personal data from a third party should be accompanied by evidence that the third party is able to act on the data subject's behalf. If this is not provided, we may contact the third party to ask that such evidence be forwarded before we comply with the request.

d) **Timescales:** Usually, we will comply with a person's request without delay and at the latest within one month. Where requests are complex or numerous, we may contact the person to inform them that an extension of time is required. The maximum extension period is two months.

e) **Fee:** We will normally comply with a data subject's request at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may contact the person requesting a fee. This fee must be paid in order for us to comply with the request. The fee will be determined at the relevant time and will be set at a level which is reasonable in the circumstances. In addition, we may also charge a reasonable fee if the person requests further copies of the same information.

f) Information a Data Subject will Receive: When a person makes a subject access request, the person will be informed of:

i. whether or not their data is processed and the reasons for the processing of their data;
ii. the categories of personal data concerning the data subject;
iii. where the data has been collected from if it was not collected from the data subject;
iv. anyone who their personal data has been disclosed to or will be disclosed to
v. how long their data is kept for (or how that period is decided);
vi. the data subject's rights in relation to data rectification, erasure, restriction of and objection to processing;
vii. a person's right to complain to the Information Commissioner if the person is of the opinion that their rights have been infringed;
viii. the reasoning behind any automated decisions taken about them.

g) **Circumstances in which a Person's Request may be Refused:** *We may refuse to deal with a data subject access request if it is manifestly unfounded or excessive, or if it is repetitive. Where it is our decision to refuse a person's request, we will contact the person without undue delay, and at the latest within one month of receipt, to inform them of this and to provide an explanation. The person will be informed of their right to complain to the Information Commissioner and to a judicial remedy.*

We may also refuse to deal a person's your request, or part of it, because of the types of information requested. For example, information which is subject to legal privilege or relates to management planning is not required to be disclosed. Where this is the case, we will inform the person that their request cannot be complied with and an explanation of the reason will be provided.

Data Breach Notification

a) **Aim:** We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely. One such obligation is to report a breach of personal data in certain circumstances and this sets out our position on reporting data breaches.

b) Personal Data Breach: ***A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.***

The following are examples of data breaches:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a data controller or data processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

c) **Investigation into Suspected Breach:** In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by the manager who will make a decision over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

d) **When a Breach will be Notified to The Information Commissioner:** In accordance with the GDPR, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical,

material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required. The following information will be provided when a breach is notified:

i. a description of the nature of the personal data breach including, where possible:
   - ⚠ the categories and approximate number of individuals concerned; and
   - ⚠ the categories and approximate number of personal data records concerned
ii. the name and contact details of the manager where more information can be obtained;
iii. a description of the likely consequences of the personal data breach; and
iv. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

e) When a Breach will be Notified to The Individual: In accordance with the GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online**.**

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

i. a description of the nature of the breach
ii. the name and contact details of the manager where more information can be obtained
iii. a description of the likely consequences of the personal data breach and
iv. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

f) Record of Breaches: The Company will be recording all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

Privacy Notice for Service Users

Kindcare (UK) Ltd, trading as Bendigo Nursing Home, in accordance with the General Data Protection regulation (GDPR) we have implemented this Privacy Notice to inform you, our residents, of the types of data we hold on you and process. This Privacy Notice also explains how we use any personal information we collect about you, during the information gathering process known as an Assessment of Need. Topics covered are:

- *What information do we collect about you?*
- *How do we use such information?*
- *Access to your information and correction*

1. **What information do we collect about you, the lawful basis of the information gathered, who provided the data and retention period?:** The nature of our service means that very personal and sensitive information is discussed, in order to ensure we can meet your health and social care needs in ways that are unique to your individual circumstances. The specific type of information is required in order for us to meet our legal and regulatory obligations as a registered provider. The Lawful Bases which we use are contained within the Data Protection Act 2018 and are:

Data / Information we hold on You	Lawful Basis	Who Provided the Information / Data	Retention Period
Name, Date of Birth	Legal Obligation	You or your LPA / POA / NOK, or Local Authority	Records are archived and kept for 3 years after the date of last entry, after which hard / paper copies are cross shredded and digital copies are deleted
Next of Kin / Relevant, Involved Family Members, LPA (Lasting Power of Attorney) / POA) contact details	Legal obligation (*involvement and decision-making*)	You or your LPA / POA / NOK, or Local Authority	
Records and contact details on relevant professionals involved in your care, treatment and support such as GP, Social Worker, Community Dietician, Optician, etc.	Legal Obligation (*co-ordinated care*)	You or your LPA / POA / NOK, or Local Authority or requested by the home	
Medical History	Legal Obligation	Your GP	
Health and Monitoring Records (including past and current weight, blood pressure, nutrition, hydration, BMI, vision, hearing, etc.)	Legal Obligation (*in meeting needs*)	Your GP or as per our assessment	
Medicines	Legal Obligation	Your GP	
Well-being (including mental, social and spiritual needs, life history and family tree, your preferences and wishes as well as end of life care wishes)	Legal Obligation (*in meeting needs in a person-centred way*)	You, your family / representative, psychiatrist / GP, our assessment	
Special Categories Data (race, ethnic origin, religion, disability, sex, sexual orientation)	Legal obligation (*to ensure equality and necessary adjustment*)	You / your representative	
Letters and documents such as hospital appointments, funeral arrangements, advance decisions, correspondence with your representative, copies of LPA / POA, signed Terms of Business and Contract, NHS letter related to Nursing needs and contribution)	Legal Obligation (*co-ordinated care*) as well as Contractual (*payments*)	You, your family / representative, LPA / POA, GP, hospital, NHS	

Photographs (such as your photograph, photographs of any pressure wounds or skin damage)	Legal Obligation (*i.e. the right medication is administered to the right person*)	Our staff	
Accidents / incidents reports	Legal Obligation	Our staff	
Complaints, issues raised and investigations	Legal Obligation	You / other complainant, manager, deputy manager	
Care Planning (current and archived)	Legal Obligation	You and our staff	
Risks and needs assessments	Legal Obligation	Our staff	
Notifications to CQC (Care Quality Commission) and other regulatory organisations	Legal Obligation	Our staff	
Feedback of our service	Legal Obligation	You	For about 12 months
Financial records (such as invoices and payments made by you / your representative / Local Authority (LA) / NHS) as well as any additional expenses	Legal Obligation (*HMRC*) as well as Performance of a Contractual	Our accounts department, you / LPA / POA, LA, NHS	6 years

2. **How information about you will be used:** We may share information regarding your care with those who have a need to know, namely Health Professionals, such as GP's, Ambulance Paramedics, Hospitals etc., Local Authorities, include departments such as Social Services, etc. and any relevant person identified by you, such as an L.P.A., and our staff. We will not share your information with anyone except those indicated above, unless required by law. Personal information supplied to us is used in a number of ways, for example.
   - To agree a Care Plan
   - To review your care needs
   - To monitor your medication
   - Share information about you with relevant professionals involved in your care, treatment and support such as GP, Hospital, Dietician, Optician, etc. in order to provide well-managed and co-ordinated care, treatment and support. For this purpose, the lawful basis are legal obligation, however, in cases where there is a lack of capacity the lawful basis changes to vital interests.
   - To help us improve our services
   - Photographs are:
     i. Used for your MAR sheets where medicines administration is recorded. We are required to administer the right medicine to the right person and having a photograph available ensure that there are no errors, and hence this is a legal obligation.
     ii. Also used to display on your room door for identification purposes and this is our legitimate interests
     iii. Used for display around the home, our TV monitors and brochure as part of you daily activities in which case we ask for your consent

3. **How will we use this information?:** Upon completion of your Assessment of Need, we compile a Care Plan with your involvement and the involvement of people you have chosen, which sets out tasks, aspirations and outcomes in order to meet all your identified needs and this is regularly reviewed and updated. This includes liaison with all those involved in your care such as family, your representative relevant health and social care colleagues and other professionals.

4. **Access to your information and corrections:** All files held in your name are available for your perusal and you can ask us to remove or amend information which is inaccurate.

5. **Protecting your Data:** We are aware of the requirement to ensure your data is protected against accidental loss or inappropriate disclosure, destruction and abuse. We have implemented processes to guard against such.

6. **Your Rights:** You have the following rights in relation to the personal data we hold on you:
   a) the right to be informed about the data we hold on you and what we do with it;
   b) the right of access to the data we hold on you.
   c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected.
   d) the right to have data deleted in certain circumstances. This is also known as 'erasure';, however, that may mean that we are unable to ensure appropriate care, treatment and support
   e) the right to restrict the processing of the data;
   f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
   g) the right to object to the inclusion of any information;
   h) the right to regulate any automated decision-making and profiling of personal data.

7. **Consent:** Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

8. **Making a Complaint:** If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

9. **Data Protection Compliance:** alternatively, you can inform the manager either verbally or in writing to Mariana, Bendigo Nursing Home, 22 Arundel Road, Eastbourne, BN21 2EL; **mariana@kindcare.co.uk**

Privacy Notice for Service Users' Relevant Persons Involved (LPA / POA, NOK, Family Members)

Kindcare (UK) Ltd, trading as Bendigo Nursing Home, in accordance with the General Data Protection regulation (GDPR) we have implemented this Privacy Notice to inform you, our residents' representatives, of the types of data we hold on you and process. This Privacy Notice also explains how we use any personal information we hold on you.

- *What information do we hold on you?*
- *How do we use such information?*
- *Access to your information and correction*

1. **What information do we collect about you, the lawful basis of the information gathered, who provided the data and retention period?:** The Lawful Bases which we use are contained within the Data Protection Act 2018 and are:

Data / Information we hold on You	Lawful Basis	Who Provided the Information / Data	Retention Period
Contact Details (full name, address, telephone number(s), e-mail address, business / law firm name, fax number)	Legal Obligation (*involve representatives in the residents' care, treatment and support under the Health and Social Care Act*)	You	Records are archived and kept safe for 3 years after the date of last entry, after which hard / paper copies are cross shredded and digital copies are deleted
Letters and correspondence (hard / paper copies and e-mails), copies of LPA / POA, signed Terms of Business and Contract on behalf of the resident	Performance of a contract	You	
Care Planning (involvement, including Best Interest Decision records, DNACPR)	Legal Obligation	You	
Records of verbal communication (either in person or on the phone)	Legal Obligation	You	
Complaints, issues raised and investigations	Legal Obligation	You / other relevant complainant(s), manager, deputy	
Feedback of our service	Legal Obligation	You	For about 12 months
Financial records (such as invoices and payments as well as any additional expenses)	Legal obligation (*HMRC*)	You and our accounts department	6 years

2. **How information about you will be used:** We will only share your contact details that you have provided willingly with Health Professionals, such as GP's, Hospitals, other professionals involved such as optician, etc., Local Authorities, include departments such as Social Services, our staff to keep you informed of the condition of the person whose care, treatment and support you are involved in, as well as our accounts department. We will not share your information with anyone except those indicated above, unless required by law.

3. **Access to your information and corrections:** Any information held on you is available to you and you can ask us to remove or amend information which is inaccurate.

4. **Protecting your Data:** We are aware of the requirement to ensure your data is protected against accidental loss or inappropriate disclosure, destruction and abuse. We have implemented

processes to guard against such.

5. **Your Rights:** You have the following rights in relation to the personal data we hold on you:
   a) the right to be informed about the data we hold on you and what we do with it;
   b) the right of access to the data we hold on you.
   c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected.
   d) the right to have data deleted in certain circumstances. This is also known as 'erasure', however, that may mean that we are unable to ensure appropriate care, treatment and support
   e) the right to restrict the processing of the data;
   f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
   g) the right to object to the inclusion of any information;
   h) the right to regulate any automated decision-making and profiling of personal data.

6. **Consent:** Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

7. **Making a Complaint:** If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

8. **Data Protection Compliance:** alternatively, you can inform the manager either verbally or in writing to Mariana, Bendigo Nursing Home, 22 Arundel Road, Eastbourne, BN21 2EL; **mariana@kindcare.co.uk**

Privacy Notice for Employees

In accordance with the General Data Protection Regulation (GDPR), we have implemented this privacy notice to inform you, our employees, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

1. **Data Protection Principles:** Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:
   a) processing is fair, lawful and transparent
   b) data is collected for specific, explicit, and legitimate purposes
   c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
   d) data is kept accurate and up to date, data which is found to be inaccurate will be rectified or erased without delay
   e) data is not kept for longer than is necessary for its given purpose
   f) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures

2. **Types of Data Held:** We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold some of the data within our computer systems. Specifically, we hold the following types of data:

Data / Information we hold on You	Lawful Basis	Who Provided the Information / Data	Retention Period	Who we Share your Data with
Personal Details (*full name, 5 years address history, telephone number(s), e-mail address, social media information*)	Legal Obligation (*for criminal check and ensure safety of service users*)	You	Records are archived and kept safe for 3 years after the date of last entry, after which hard / paper copies are cross shredded and digital copies are deleted	• DBS check • Payroll • HMRC • Pension Scheme • CQC • Immigration
Name and contact details of your next of kin	Vital interests	You		Emergency services such as ambulance, police, etc.
Name and contact details of your GP	Vital interests	You		
Gender, marital status, disability	Legal obligation (*equality*)	You		Not shared, unless there are legally required to provide information for equality purposes
Children and child care	Legal obligations (*to determine reasonable adjustments*)	You		HMRC, payroll
Health and medical condition, including vaccinations	Legal obligations (*fitness for work*)	You		Emergency services such as ambulance or for the prevention of infection

	Your photograph	Legitimate Interests	You		• for your file • for ID badge • for your locker • some marketing purposes with a consent
	Copies of ID (*such as passport, ID card, driving licence*)	Legal obligation (*for DBS checks and immigration / right to work purposes*)	You	Records are archived and kept safe for 3 years after the date of last entry, after which hard / paper copies are cross shredded and digital copies are deleted	• for DBS / criminal checks • for immigration / the right to work / UK Border Agency • CQC • NMDS - SC
	Right to work in the UK / immigration / sponsorship licence	Legal obligation	You and / or us / the employer		
	Criminal convictions / DBS records	Legal obligation	Obtained by the employer		CQC
	Special categories of data (*race, ethnic origin, sex life, sexual orientation, religion, genetic and biometric data*)	Legal obligation (*equality and non-discrimination*)	You		NMDS – SC and if there is legally required to provide information for equality purposes
	Information gathered via recruitment (*such as data provided by you on your CV, application form, cover letter, interview notes*)	Legal obligation (*robust recruitment procedures*)	You		CQC
	Minimum 2 references from previous employers	Legal obligation	You and obtained by the employer		CQC
	Details and evidence on education, professional training, employment history, professional organisations membership such as NMC	Legal obligation (*robust recruitment procedures*)	You and verified by the employer		• CQC • NMDS - SC
	National Insurance Number	Legal Obligation (*HMRC*)	You	6 years	• HMRC • payroll • CQC • NMDS – SC
	Tax Code	Legal Obligation (*HMRC*)	You	6years	• HMRC • payroll
Information related to your employment with us	Job title and job description	Performance of Contract	Both parties: you and employer	3 years	• Payroll • CQC • NMDS - SC
	Financial (*Your rate of pay / hours worked / payroll / pension / benefits, SMP, SSP, SPP, certificates, timesheets)*	Legal Obligation (*HMRC*)	Both parties agreed: you and employer	6 years, for pension: 6 years after the ending of any benefit payable	• Payroll • HMRC • Pension company • NMDS – SC • CQC

	Terms and conditions of employment / contract	Performance of Contract	Both parties agreed: you and employer	3 years	Not shared, unless there is a tribunal dispute and lawyers may be involved or other third party
	Internal and external training undertaken	Legal Obligation	Both parties agreed: you and employer		CQC NMDS - SC
	Information on sickness absence, family leave	Performance of Contract	Both parties agreed: you and employer	3 years	Payroll
	Information on annual leave	Performance of Contract	Both parties agreed: you and employer	6 years	Payroll
	Details of formal and informal proceedings (*such as letters of concern, disciplinary and grievance proceedings, appraisal and supervision records and agreed personal development plans*)	Legal obligation	Both parties agreed: you and employer, as well as a third party or other organisations involved	3 years	CQC or if a formal dispute, with lawyers or other third party, ACAS
	Feedback	Legal obligation	You	About 12 months	Feedback is anonymised and evaluated results are shared with residents, their representatives and CQC
	Duty rotas	Legal obligation	Manager / deputy manager	4 years	All staff and CQC
	IT equipment use, including telephone and internet access	Legitimate Interests	Manager	Cancel straight away when employ-ment is terminated	Not shared

3. **Failure to Provide Data:** Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you. This could include being unable to offer you employment, or administer contractual benefits.

4. **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.

5. **Employee Rights:** You have the following rights in relation to the personal data we hold on you:
   a) the right to be informed about the data we hold on you and what we do with it;
   b) the right of access to the data we hold on you.
   c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
   d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
   e) the right to restrict the processing of the data;

f) the right to transfer the data we hold on you to another party. This is also known as ‘portability’;
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.

6. **Consent:** Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

7. **Making A Complaint:** If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

8. **Data Protection Compliance:** alternatively, you can inform the manager either verbally or in writing to Mariana, Bendigo Nursing Home, 22 Arundel Road, Eastbourne, BN21 2EL; mariana@kindcare.co.uk

Privacy Notice for Job Applicants

In accordance with the General Data Protection Regulation (GDPR), we have implemented this privacy notice to inform you, our employees, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

6. **Data Protection Principles:** Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:
   g) processing is fair, lawful and transparent
   h) data is collected for specific, explicit, and legitimate purposes
   i) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
   j) data is kept accurate and up to date, data which is found to be inaccurate will be rectified or erased without delay
   k) data is not kept for longer than is necessary for its given purpose
   l) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures

7. **Types of Data Held:** We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold some of the data within our computer systems. Specifically, we hold the following types of data:

Data / Information we hold on You	Lawful Basis	Who Provided the Information / Data	Retention Period	Who we Share your Data with
Personal Details (*full name, telephone number(s), e-mail address, social media information*)	Legitimate Interest	You	Records are archived and kept safe for 3 months after the date of last entry, after which hard / paper copies are cross shredded and digital copies are deleted	Not shared, unless there is a dispute
Gender, marital status, disability	Legal obligation (*equality and to make reasonable adjustments*)	You		Not shared, unless there is legally required to provide information for equality purposes
Children and child care	Legal obligations (*to determine reasonable adjustments, i.e flexible working hours*)	You		Not shared
Copies of ID (*such as passport, ID card, driving licence*)	Legal obligation (*immigration / right to work in the UK*)	You		for immigration / the right to work / UK Border Agency
Right to work in the UK / immigration / sponsorship licence	Legal obligation	You and / or us / the employer		
Special categories of data (*race, ethnic origin, sex life, sexual orientation, religion, genetic and biometric data*)	Legal obligation (*equality and non-discrimination*)	You		if there are legally required to provide information for equality purposes

Information gathered via recruitment (*such as data provided by you on your CV, application form, cover letter, interview notes*)	Legal obligation (*robust recruitment procedures*)	You		Not shared at this stage
Minimum 2 references from previous employers	Legal obligation	You and obtained by the employer		Not shared at this stage
Details and evidence on education, professional training, employment history, professional organisations membership such as NMC	Legal obligation (*robust recruitment procedures*)	You and verified by the employer		Not shared at this stage
Job title and job description	Performance of Contract	Both parties: you and employer		Not shared at this stage

8. **Failure to Provide Data:** Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you. This could include being unable to offer you employment, or administer contractual benefits.

9. **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.

10. **Employee Rights:** You have the following rights in relation to the personal data we hold on you:
    i) the right to be informed about the data we hold on you and what we do with it;
    j) the right of access to the data we hold on you.
    k) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
    l) the right to have data deleted in certain circumstances. This is also known as 'erasure';
    m) the right to restrict the processing of the data;
    n) the right to transfer the data we hold on you to another party. This is also known as 'portability';
    o) the right to object to the inclusion of any information;
    p) the right to regulate any automated decision-making and profiling of personal data.

9. **Consent:** Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

10. **Making A Complaint:** If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

11. **Data Protection Compliance:** alternatively, you can inform the manager either verbally or in writing to Mariana, Bendigo Nursing Home, 22 Arundel Road, Eastbourne, BN21 2EL; mariana@kindcare.co.uk

Related Policies

Adult Safeguarding
Accessible Information and Communication
Access to Records
CCTV
Confidentiality
Consent
Cyber Security
Duty of Candour
Record Keeping

Related Guidance

- Smaller Organisations ICO https://ico.org.uk/for-organisations/business/
- Your privacy Notice Checklist https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/your-privacy-notice-checklist/
- Guide to the general data Protection Regulations (GDPR) https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- Guide to the Privacy and Electronic Communications May 2016 Regulations https://ico.org.uk/media/for-organisations/guide-to-pecr-2-3.pdf
- Records Management Code of Practice for Health and Social Care 2016 https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016
- ICO Code of practice on privacy notices, transparency and control
- https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf
- ICO Data protection Self-Assessment https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/
- Direct Marketing Guidance https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf
- Data Protection Fees Information Commissioner https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/02/new-model-announced-for-funding-the-data-protection-work-of-the-information-commissioner-s-office/
- Example of Privacy Notice https://www.johnlewis.com/customer-services/shopping-with-us/privacy-notice
- Guide to privacy and Electronic Communications Regulations (PECR) https://ico.org.uk/for-organisations/guide-to-pecr/
- Data Protection and the use of criminal offence data for employment and education purposes August 2018: **https://www.nacro.org.uk/wp-content/uploads/2018/08/Nacro-briefing-Data-protection-and-the-use-of-criminal-offence-data.pdf**