General Data Protection Regulation (GDPR) Policy

Policy Statement

Bright Care is committed to conducting its business in accordance with all Data Protection laws and regulations, and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of Bright Care employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a Bright Care contact (i.e. the Data Subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as Data Controller. Bright Care, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose Bright Care to complaints, regulatory action, fines and/or reputational damage.

Bright Care is fully committed to ensuring continued and effective implementation of this policy and expects all employees and Third Parties to share this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

Scope

This policy has been designed to establish standards for the processing and protection of personal data by Bright Care.
This policy applies to all Bright Care's activities where a data subject's personal data is processed:

- In the context of the company's activities
- For the provision or offer of services to individuals by Bright Care
- To actively monitor the behaviour of individuals
- Monitoring the behaviour of individuals using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to:
  - Taking a decision about them
  - Analysing or predicting their personal preferences, behaviours and attitudes.
    This policy applies to all processing of personal data in electronic form or where it is held in manual files.

Definitions

- Employee – an individual who works for Bright Care, under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. This includes temporary employees and independent contractors.
- Contact – any past, current or prospective Bright Care client or customer.
- Third Party – an external organisation with which Bright Care conducts business and is also authorised to, under the direct authority of Bright Care, process data or Bright Care contacts.

- Consent – any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- Personal Data – any information (including opinions and intentions) which relates to an identified or identifiable natural person. "Personal data" is defined as any information relating to a person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- Identifiable Natural Person – anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- Data Subject – the identified or identifiable natural person to which the data refers.
- Process, Processed, Processing – any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Operations performed may include 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 Controller – a controller is a natural or legal person, public authority or agency that decides the purpose and manner that personal data is used, or will be used.
- Data Processors – a processor is a group or a natural or legal person, public authority or agency that processes the data on behalf of the controller. Processing is obtaining, recording, adapting or holding personal data
- Supervisory Authority – an independent public authority responsible for monitoring the application of the relevant data protection regulation set forth in law.
- Data Protection – the process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.
- Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- Special Categories of Data – personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- Profiling – any form of automated processing of personal data where personal data is used to evaluate specific or general characteristics relating to an Identifiable natural person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Responsibilities

Compliance with the legislation is the personal responsibility of Bright Care employees who process personal information.

Responsibilities under the terms of GDPR are:

1. Bright Care is the 'Data Controller' – this means it is ultimately responsible for controlling the use and processing of the personal data.

2. Bright Care's Management Team are the 'Data Processors' - this means they process data on behalf of the Data Controller. Bright Care Data Processors are responsible for all day-to-day data protection matters; processing, obtaining, recording, adapting or holding personal data. They are also responsible for ensuring that all Bright Care employees and relevant individuals abide by this policy, and for developing and encouraging good information handling within the company.

3. Bright Care's Supervisory Authority is the Information Commissioners Office (ICO). Bright Care must notify the Supervisory Authority of any breaches of data. Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of ICO. The nature of the breach or loss can then be considered together with whether the data controller is properly meeting his responsibilities under the legislation. 'Serious breaches' are not defined. Our data registration number with the Supervisory Authority: ICO Security number**:** CSN7690862

4. Bright Care appoints Jemima Vertha, Business Manager, who is available to address any concerns regarding the data held by company and how it is processed, held and used. Jemima is also responsible for ensuring that Bright Care's notification to the Supervisory Authority is kept reported and accurate in detail.

Data Protection Principles

The legislation places a responsibility on every Data Controller to process any personal data in accordance with the stated principles. Bright Care applies the principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

- **Principle 1: Lawfulness, Fairness and Transparency** - Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, Bright Care must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).
- **Principle 2: Purpose Limitation** - Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means Bright Care must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.
- **Principle 3: Data Minimisation** - Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

This means Bright Care must not store any personal data beyond what is strictly required.

- **Principle 4: Accuracy** - Personal Data shall be accurate and, kept up to date. This means Bright Care must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.
- **Principle 5: Storage Limitation** - Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. (see Data Retention section)
  This means Bright Care must, wherever possible, store personal data in a way that limits or prevents identification of the data subject. Bright Care must not retain personal data for longer than necessary to ensure compliance with this legislation. This means Bright Care must undertake regular reviews of the information held and implement a 'weeding' process.
- **Principle 6: Integrity & Confidentiality -** Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. This means, Bright Care must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times. Bright Care will only process data in accordance with individuals' rights.
- **Principle 7: Accountability** - The Data Controller shall be responsible for and be able to demonstrate compliance. This means Bright Care must demonstrate that the six Data Protection Principles (outlined above) are met for all personal data for which it is responsible.

Data Protection

Bright Care adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a data processor, the data can be processed only in accordance with the instructions of the data controller.
- Ensure that personal data is protected against undesired destruction or loss.

- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary.

Data Consent

Bright Care understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement.
Bright Care will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned.
Bright Care has established a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data. The system includes provisions for:

- Determining what disclosures should be made in order to obtain valid consent.
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the consent is freely given (i.e. is not based on a contract that is conditional to the processing of personal data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the consents given.
- Providing a simple method for a data subject to withdraw their consent at any time.

Bright Care will ensure that any forms used to gather data on an individual will contain a statement explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

Bright Care's specimen consent statement is:

At Bright Care, we take your privacy seriously. Here's our consent form in which we ask for your permission to collect, store and use any appropriate personal information that you give us.

What Information Does Bright Care Collect, Store and Use:

- *We collect the minimum amount of personal information in order to provide our services.*
- *We may also collect information obtained from cookies or tracking technologies on our website.*
- *We hold your personal information securely in our cloud-based systems, or office-based archives.*
- *We use this personal information (particularly your contact details and ID photo for carers), solely for communicating with you on subjects related to your relationship with Bright Care. For example, company updates, invoicing, or pay etc.*
- *We do not sell or hire out your data. We only share relevant personal information with appropriate people involved in your relationship with Bright Care, i.e. details of a care package. Your details are also stored on some third-party services who help us provide our services.*

Entitlement To View Your Information
You are entitled (on request, and without charge) to receive a copy of the information that we hold about you, and to have any inaccuracies corrected or deleted. You can also request a full copy of our GDPR Policy.
Please contact Bright Care at: Tower Mains, 18C Liberton Brae, Edinburgh, EH16 6AE or on 0131 344 4670 if you wish to exercise this right. You can also email: info@brightcare.co.uk.

Consent And Withdraw
The legal basis for us to process your personal information is by consent, i.e. we require you to complete this consent form. If you withdraw consent at any time, we will immediately delete the information you have given us from our records. Please use the contact information as above to do so.

Bright Care also receives consent for processing data from contacts via the company's online programmes which display consent declarations such as *"I understand that my application and respective data will be processed under Bright Care's GDPR Policy that can be requested at any time."*
Bright Care will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Data Processing

Bright Care uses the personal data of its contacts for the following broad purposes:

- The general running and business administration of the company.
- To provide services to Bright Care's customers.
- The ongoing administration and management of customer services.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.
Bright Care will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, Bright Care will not process personal data unless at least one of the following requirements are met:

1. The data subject has given consent to the processing of their personal data for one or more specific purposes.
2. Processing is necessary for the performance of providing an agreed service to which the data subject is party or in order to take steps at the request of the data subject prior to entering into an agreed service.
3. Processing is necessary for compliance with a legal obligation to which the data controller is subject.
4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

Special Categories of Data

Bright Care will only process special categories of data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.

- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

In any situation where special categories of data are to be processed, prior approval must be obtained from the Supervisory Authority Contact Person, Jemima Vetha, and the basis for the processing clearly recorded with the personal data in question.

Subject Access Rights & Requests

Individuals have a right to access any personal data relating to them which are held by Bright Care. Any individual wishing to exercise this right should notify the Branch Manager who will make the necessary arrangements to make the data readily available at an agreed date and time. Under the terms of the legislation, any such requests must be complied with within 40 days.

Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime; including Adult Support and Protection subjects
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the order of a court or by any rule of the law or legislation pertaining to the company's activities.

If Bright Care processes personal data for one of these purposes, then it may apply an exception to the processing rules outlines in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

Disclosure of Data

Bright Care undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police. Legitimate disclosures may occur in the following instances:

- The individual has given their consent to the disclosure.
- The disclosure has been notified to the Supervisory Authority and is in the legitimate interests of the individual.
- In emergency circumstances and is in the best interest of the individual to protect them from harm or abuse.
- In circumstances where the individual is subject to adult support and abuse procedures as per our regulatory bodies guidance.

In no circumstances will Bright Care sell any of it's databases to a third party.

Data Quality

Bright Care take all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject.

The measures adopted by the company to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
  - a law prohibits erasure.
  - erasure would impair legitimate interests of the data subject.

Data Retention

To ensure fair processing, personal data will not be retained by Bright Care for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

The length of time for which Bright Care needs to retain personal data is set out in the Bright Care 'Personal Data Retention Schedule', as follows:

- Lead customer enquiries – retained for maximum period of 1 year
- Declined employee applicants – retained for maximum period of 3 years
- Finished employees – retained for maximum period of 7 years
- Finished clients/customers – retained for maximum period of 7 years

This takes into account the legal, contractual and regulatory requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection Breaches

Bright Care has a duty to report certain types of personal data breaches to the Supervisory Authority to which it is registered. Bright Care hold registration with the Information Commissioners Office (ICO). Notification responsibility is undertaken by Bright Care's main registered contact person with ICO. Our data registration number with the Supervisory Authority is: CSN7690862

The procedure is as follows:

- Bright Care' must report serious breaches to ICO within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the company must also inform those individuals without undue delay.
- Bright Care must have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not there is a need to notify the relevant supervisory authority and the affected individuals.

- Bright Care must keep a record of any personal data breaches, regardless of whether they are subject to notifications or not.
- Bright Care must learn from breaches and put in place preventative measures to eliminate a recurrence of the breach.

Publication of Company Information

Bright Care publishes various items which will include some personal data; for example:

- internal telephone directory
- event information
- photos and information in marketing materials

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted personnel access only. Therefore it is Bright Care's policy to request completion of a Consent Form (see Appendix 1) and offer an opportunity to opt-out of the publication of such when collecting the information.

Marketing

Bright Care will not send promotional or marketing material to a contact through digital channels such as mobile phones, email and the internet, without first obtaining their consent.

Where personal data processing is approved for marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the data subject puts forward an objection, marketing related processing of their personal data will cease immediately, and their details will be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

External Privacy Notices

Bright Care's external website includes an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law. Please see Appendix 2

Email

It is the policy of Bright Care to ensure that senders and recipients of email are made aware that under the Data Protection Act, and Freedom of Information Legislation, the contents of email is confidential. may have to be disclosed in response to a request for information. One means by which this is communicated, is by a disclaimer on company email signatories:

The information contained in this email is confidential and is intended solely for the individual or entity to whom it is addressed. If you received this message in error or are not the intended recipient, you should destroy the email message and any attachments or copies, and you are prohibited from retaining, distributing, disclosing or using any information contained herein. Please inform us of the erroneous delivery by return email. Thank you for your cooperation.

Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) and Data Protection Act 1998. Please follow this link to the Supervisory Authority website; ICO (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website. For help or advice on any data protection or freedom of information issues, please do not hesitate to Jemima Vetha, Business Manager, Bright Care.

Data Protection Training

Bright Care personnel have a good understanding of the new GDPR law and are continually informed, communicated with and trained.

Bright Care's Data Processors (the Management Team), undertake formal company training on GDPR and company procedures and processes in relation to this. The training provides Data Processors with clear instruction as to their responsibilities for all day-to-day data protection matters.

Bright Care's employees (non-management), will also company training to provide general understanding of GDPR and their responsibilities related to their role.

APPENDIX 1

Bright Care Consent Form

At Bright Care, we take your privacy seriously. Here's our consent form in which we ask for your permission to collect, store and use any appropriate personal information that you give us. There are two independent sections.

SECTION A: INTERNAL USAGE

What Information Does Bright Care Collect, Store and Use

- We collect the minimum amount of personal information in order to provide our services.
- We may also collect information obtained from cookies or tracking technologies on our website.
- We hold your personal information securely in our cloud-based systems, or office-based archives.
- We use this personal information (particularly your contact details or ID photo for carers), solely for communicating with you on subjects related to your relationship with Bright Care. For example, company updates, invoicing, or pay etc.
- We do not sell or hire out your data. We only share relevant personal information with appropriate people involved in your relationship with Bright Care, i.e. details of a care package. Your details are also stored on some third-party services who help us provide our services.

Entitlement To View Your Information

You are entitled (on request, and without charge) to receive a copy of the information that we hold about you, and to have any inaccuracies corrected or deleted. You can also request a full copy of our GDPR Policy.

Please contact Bright Care at: Tower Mains, 18C Liberton Brae, Edinburgh, EH16 6AE or on 0131 344 4670 if you wish to exercise this right. You can also email: info@brightcare.co.uk.

Consent And Withdraw

The legal basis for us to process your personal information is by consent, i.e. we require you to complete this consent form. If you withdraw consent at any time, we will immediately delete the information you have given us from our records. Please use the contact information as above to do so.

I have read, understand, and consent to the above information.

Full Name	Signature	Date

SECTION B: EXTERNAL USAGE

It can be really useful for Bright Care to take photos or videos at events to publicise our activities. This section is about whether or not you'd be happy for us to use photographs of you for any marketing or external use.

What Photographs Does Bright Care Collect, Store and Use

- We may take photographs at event or activities.
- We may use your photographs on our social media accounts (such as Facebook or LinkedIn), on our website, or within company newsletters.

I have read, understand, and consent to the above information.

Full Name	Signature	Date

APPENDIX 2

Privacy Notice and Cookie Notice

Bright Care At Home Limited (Bright Care At Home, “we”, or “us”) takes your privacy seriously. Here’s our privacy policy, which covers in detail the information we collect, how we use it to improve your experience, and how we keep this information secure.

This Privacy Policy applies to Bright Care’s owned and operated websites, and does not apply to the practices of companies that Bright Care does not own or control, or to people that Bright Care does not employ or manage.

There are links within the pages of Bright Care which lead to other websites; please make sure you read the privacy policy of any other sites that may ask for personally identifiable information before you register with them.

What Information Does Bright Care Collect?

Bright Care collects the minimum amount of personally identifiable information it possibly can in order to provide a great service to its customers. The data collected can be traced back to three scenarios:

i. Personal Details

When you contact us through our website, live-chat, application forms or applying for one of our services, we collect your first name, surname, address, telephone number and e-mail address. None of our customers’ data is made public.

ii. Cookies and Tracking Technologies

This type of information is automatically collected when a user visits our website through the use of cookies, beacons, tags, and scripts. The data retrieved includes IP address, browser type, pages requested, referring/exit pages and URLs, number of clicks, landing pages and other data of this nature. We do not link this automatically-collected data to personally identifiable information.

iii. Email

When we communicate via email, we also keep record of your interactions with the email, including whether you have opened it, and what links have been clicked.

How Does Bright Care Use Your Information?

In short, we use your information to customise and improve your Bright Care experience. We use the information collected in a variety of ways, including:

i. Enhanced Experience

We use your data to provide you with the services you have requested from us or have expressed an interest in (for example, our care worker opportunities, or tips for caring

for the elderly), as well as carry out profiling and market research. This data is used to improve your experience and help us to better understand and respect your preferences.

ii. Communications

We use your data to communicate with you about our services, community news and updates. The use of personal data ensures we can customise our messages, and also tailor them to reflect your interests and preferences.

iii. Analytics

We use Google Analytics to measure and track your journey through our website. This is used to understand how visitors use our platform and ultimately, to help us deliver a better experience, more relevant content and more customised communications. Please note that Google operates independently from us and has its own privacy policy.

How Do We Share Your Information?

Bright Care will not sell, share or hire out data; we are the sole owner of the information collected on this site. However, we may send personally identifiable information to other companies or individuals when:

i. We need to share the information to provide a service you have requested.

ii. We need to send the information to member companies who work on behalf of Bright Care to provide a service to you (unless we tell you differently, these companies do not have the right to use the personally identifiable information we provide to them beyond what is necessary to assist us).

iii. In the unlikely event of having to respond to legal summonses, court order or other legal processes.

How Can You Opt-Out From Commercial Communications?

There are no pre-ticked boxes on our website and, where practicable, we operate a double opt-in process to ensure that we have properly obtained your consent to store and use the personal information.

Our customers and users of our website are given the opportunity to opt out of having information sent to them at the time of registration. If you later wish to change this option, you may contact us to request that your name be taken off our contact list. We also include an opt-out or unsubscribe link at the bottom of every email we send.

What Are Your Rights Regarding Data?

As an individual, you have the right to: be informed about our use of your data; access your personal data; rectify your data if it is inaccurate or incomplete; request the deletion of your personal data; restrict and object to the processing of your personal data for direct marketing or research purposes, and obtain and reuse your personal data for your own purposes.

If you wish to exercise any of the above-mentioned rights, please contact Bright Care with your request.

Changes To This Policy

Bright Care may amend this policy from time to time to take into account developments in the site and changes to information collected. If we make substantial changes in the way we use your personal information, we will notify you by posting a prominent announcement on our pages.

Should you have any queries regarding the capture, storage and use of personal information by Bright Care, please don't hesitate to contact us.