Data protection/ GDPR policy

Handling personal data in line with the requirements of the GDPR

Nick Banister-Dudley, Head of Compliance and Data Protection Officer

Policy number	ALL/NBD/OPS/72
Version number	1.0
Date of issue	29/04/2021
Date for review	28/04/2024
Author	Head of Compliance and Data Protection Officer
Ratified	Care Quality, Governance and Compliance Director and Senior Information Risk Owner
Outcome	Team members will be aware of their responsibilities in respect of processing personal data under the UK GDPR and will be familiar with the steps to take to manage a data subject access request and know how to obtain specialist advice from the Data Protection Officer.
Cross reference	• Individual Rights and Data Access policy • Individual Rights and Data Access procedure • Data and IT security • Personal Data Breach policy • Records Management and Retention policy • BYOD policy • Appropriate policy document • CCTV policy • Consent for inclusion in marketing activities policies
References	• *The General Data Protection Regulation* • *Data Protection Act 2018* • *The Privacy and Electronic Communications (EC Directive) Regulations 2003* • *Guide to the General Data Protection Regulation (GDPR) (Information Commissioner's Office, accessed on 12/01/2021)* • *Guidance on Direct Marketing (Information Commissioner's Office, accessed on 12/01/2021)*

To ensure that this policy is relevant and up to date, comments and suggestions for additions or amendments are sought from users of this document. To contribute towards the process of review, email dpo@hallmarkcarehomes.co.uk

Contents

Equality and Diversity Statement

Hallmark Care Homes, Santhem Residences and Santhem Care is committed to the fair treatment of all regardless of age, colour, disability, ethnicity, gender, nationality, race, religious or spiritual beliefs, and responsibility for dependents, sexual orientation, or any other personal characteristic.

Hallmark Care Homes' Vision

To be recognised as the leading provider of high quality, relationship-centred care for all residents.

Santhem Residences' Vision

To provide exceptional environments creating peace of mind, a life of freedom & discovery at a time that is right for all.

1. INTRODUCTION

On 25 May 2018 the General Data Protection Regulation (GDPR) came into force, across the EU and applies to the UK.

The policy below provides team members with an opportunity to familiarise themselves with the requirements in respect of processing personal data under the GDPR. Having this understanding is of vital importance to ensure we can demonstrate compliance with the terms of the GDPR and avoid the risk of non-compliance fines.

We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The organisation is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

2. DEFINITIONS

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.

Controller: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all personal data relating to team members and personal data used in our business for our own commercial purposes.

Criminal Offence Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the processing of personal data.

Data Protection Officer (DPO): this term means an individual or entities whose role it is to assist the controller, to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. The DPO for Hallmark Care Homes, Santhem Residences and Santhem Care is Nick Banister-Dudley, Head of Compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Information Commissioner's Office (ICO): The ICO is the UK's independent body set up to uphold information rights. The ICO has both responsibility for ensuring the UK GDPR (and other legislation/regulations) are upheld, as well as responding to concerns from data subjects.

Personal data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

The Privacy and Electronic Communications Regulations (PECR): These sit alongside the Data Protection Act and the UK GDPR and give people specific privacy rights in relation to electronic communications.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to data subjects when we collect information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, team privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

Processing or Process: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: policies, operating procedures or processes related to this policy and designed to protect personal data. See page 2 of this policy.

Special category data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

UK GDPR: the General Data Protection Regulation ((EU) 2016/679) is legislation of the European Union that makes personal data subject to the legal safeguards specified in the GDPR. At the end of the UK-EU transition period, the General Data Protection Regulation (GDPR) forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (EUWA) (retained EU law). Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) (DP Brexit Regulations) amends the retained EU law version of the GDPR. Schedule 2 amends the Data Protection Act 2018 (DPA 2018), including that it replaces the definition of the "GDPR" in the DPA 2018 with a definition of the "UK GDPR".

3. PURPOSE OF THE POLICY

This policy sets out how we collect, process and store personal data, in line with the requirements of the UK GDPR and Data Protection Act.

4. DUTIES

The Executive Leadership Team are ultimately responsible for ensuring all team members comply with this policy and understand the need to implement appropriate practices, processes, controls and training to ensure that compliance with the requirements of the GDPR is achieved and maintained.

Each General Manager (or equivalent) is responsible for implementing this policy within their home, ensuring they understand the content of the policy, for attending relevant training and for ensuring their team members attend/complete training commensurate to their role.

The Hallmark Head of Learning and Development is responsible for ensuring team members receive training commensurate to their role so that compliance with the requirements of the GDPR can be assured.

The Regional Operations support team i.e., Operations Directors, Regional Managers, Regional Development Manager and Regional Care Specialists are responsible for ensuring their own understanding of this policy and ensuring appropriate escalation of queries and concerns to the Data Protection Officer (DPO).

The DPO is responsible for overseeing this policy and, as applicable, developing related policies and privacy guidelines.

Please contact the DPO with any questions about the operation of this policy or about the requirements of the GDPR or if you have any concerns that this policy is not being, or has not been, followed. In particular, you must always contact the DPO in the following circumstances:

- If you need to rely on consent and/or need to capture explicit consent.
- If you are unsure about what security or other measures you need to implement to protect personal data.
- If there has been a personal data breach.
- If you need to transfer data out of the UK.
- If a data subject has made a request to invoke any of their rights.
- If you are engaging in a new, or different, processing activity.
- If you plan to use personal data for purposes other than what it was collected for.
- If you plan to undertake any activities involving automated processing including profiling or automated decision-making.
- If you are commencing direct marketing.
- If you need to share data with a third party or a new data processor.

5. SCOPE OF THE POLICY

The content of this policy will apply across the entire Hallmark Care Homes Group. This includes all Hallmark care homes, the Hallmark Care Homes Central Support office, Santhem Residences and Santhem Care. Where the terms ‘organisation’ or ‘company’ are used throughout this policy, they should be read to include all the companies or business areas mentioned in this section.

All team members across the organisation will be required to act in accordance with the contents of this policy. This policy sets out what we expect from team members, to comply with applicable law. Team members compliance with this policy is mandatory. Related policies and privacy guidelines are available to help team members interpret and act in accordance with this policy and team members must also comply with all such related policies and privacy guidelines. Any breach of this policy may result in disciplinary action.

This policy must be used in conjunction with the other policies highlighted in the cross references section of this document on page 2. Copies of these policies are available on the E-learning portal.

6. SPECIFIC DETAILS

6.1 Data protection principles

Article 5 of the UK GDPR states that 7 key data protection principles, which must lie at the heart of any organisation's data protection management regime. The ICO confirms that article 5(1) requires personal data to be:

a) *processed lawfully, fairly and in a transparent manner (i.e., lawfulness, fairness and transparency);*
b) *collected only for specified, explicit and legitimate purposes (i.e. purpose limitation);*
c) *adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (i.e. data minimisation);*
d) *accurate and where necessary kept up to date (i.e. accuracy);*
e) *not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (i.e. storage limitation);*
f) *Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (i.e. security, integrity and confidentiality);*
g) *not transferred to another country without appropriate safeguards being in place (i.e. transfer limitation); and*
h) *made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data (i.e. data subject's rights and requests).*

The principles in the UK GDPR underpin all subsequent obligations and are a fundamental part of demonstrating good data protection practice. Each principle is covered separately, in the subsequent subsections.

6.1.1 Lawfulness, fairness and transparency

This principle requires that any processing of data should be lawful, fair and transparent. Whilst they overlap, all 3 elements must be satisfied when processing personal data.

Lawfulness

For the processing of personal data to be lawful, a specific ground ('lawful basis') must be identified. Article 6 of the UK GDPR defines the 6 lawful bases and the ICO provides the following explanation of each:

a) *Consent: the individual has given clear consent for you to process their personal data for a specific purpose.* See the Consent for inclusion in marketing activities policies for more information on consent.
b) *Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.*
c) *Legal obligation: the processing is necessary for you to comply with the law.*
d) *Vital interests: the processing is necessary to protect someone's life.*
e) *Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.*

f) *Legitimate interests: the processing is necessary for your 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.*

Where the lawful basis of legitimate interests is used as the lawful basis for processing, a legitimate interest's assessment will be completed by the DPO prior to the processing commencing. This three-part assessment, based on the ICO's guidance, ensures that the identified processing will be lawful.

All new processing will be discussed with, and approved by, the DPO prior to it commencing. The DPO will ensure that the organisation's record of processing document (see section 6.2.1) is updated, and the necessary assessments are completed.

Under the UK GDPR, extra levels of protection are afforded to special category (in Article 9) and criminal offence data (in Article 10). If processing special category data, both a lawful basis and a special category condition for processing must be identified. For criminal offence data, both a lawful basis and either 'official authority' or a separate condition for processing this data should be identified. All of this information, in addition to being included in the record of processing document, will be captured in the Appropriate Policy document.

In addition to the identifying a lawful basis, the lawfulness principle also requires that personal data is not managed unlawfully, in a more general sense e.g., a breach of a duty of confidence. If data has been processed unlawfully, the UK GDPR gives data subjects the right to erase the data or restrict the processing of it (see section 6.1.8).

It is also unlawful, under section 170 of the Data Protection Act 2018, to obtain personal information to use for your own aims, without either the prior consent or the knowledge of the data controller.

Fairness

The requirement of the fairness principle is that data is only processed in ways that data subjects would reasonably expect and not processed in ways that would have an unjustified negative impact on them. It is also important that data subjects are not misled when their personal data is obtained.

The DPO, when reviewing the organisation's data processing activities, will not just determine whether data can be used but also whether it should be.

Transparency

The transparency principle is fundamentally linked to the principle of fairness. The principle requires us to be clear, open and honest with data subjects about who we are, how their personal data is used and why.

This means that data subjects must be informed about the personal data we process about them. This is linked to the right to be informed (see section 6.1.8 below and the Individual

Rights and Data Access policy and procedure for more information). The information provided to data subjects must be concise, transparent, intelligible, and easily accessible. Data subjects are informed through privacy notices, policies or statements. These can be overarching documents, or just-in-time notices which inform data subjects just prior to the processing commencing.

All privacy information will be reviewed annually, or sooner should there be a change to the way in which the data is processed. If we plan to use personal data for a new purpose, we will update our privacy information and will make this available to data subjects, before starting any new processing.

6.1.2 Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. Personal data cannot be used for new, different or incompatible purposes from that disclosed when it was first obtained, unless the new purpose is compatible with the original purpose, we have informed the data subject of the new purposes and they have consented, where necessary or there is a clear legal provision requiring/allowing the processing in the public interest.

When deciding whether a new purpose is compatible with an original purpose, the ICO advises that we take into account:

- *'any link between your original purpose and the new purpose;*
- *the context in which you originally collected the personal data – in particular, your relationship with the individual and what they would reasonably expect;*
- *the nature of the personal data – e.g. is it particularly sensitive;*
- *the possible consequences for individuals of the new processing; and*
- *whether there are appropriate safeguards - e.g. encryption or pseudonymisation'.*

In short, if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is unlikely to be compatible with the original purpose.

As with the new processing of personal data, team members should speak to the DPO about using existing personal data for new purposes, prior to doing so. The DPO needs to authorise all requests of this nature before they can commence.

6.1.3 Data minimisation

The ICO is clear that data controllers must ensure the personal data they are processing is:

- *'adequate – sufficient to properly fulfil your stated purpose;*
- *relevant – has a rational link to that purpose; and*
- *limited to what is necessary – you do not hold more than you need for that purpose'.*

This means that only the minimum amount of data required to fulfil the identified purpose, should be held and processed. When personal data is no longer needed for specified purposes, it should be deleted or anonymised.

6.1.4 Accuracy

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

Personal data we use, and hold should be accurate, complete, kept up to date and relevant to the purpose for which we collected it. The accuracy of any personal data should be checked at the point of collection and at regular intervals afterwards. Everyone must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

Whilst the data held must be accurate, it is acceptable to keep records relating to mistakes. However, these records must be clear that a mistake was made and identify the corrective action taken in response to this.

6.1.5 Storage limitation

Personal data which allows for the identification of data subjects, should not be kept for longer than is necessary to meet the identified processing purpose(s).

The record of processing document states the retention periods/timescales for all the data we process. These should be adhered to, by each team member, at all times. Team members will take all reasonable steps to destroy, erase or anonymise all personal data that we no longer require in accordance with our retention timescales. This includes requiring third parties to delete that data where applicable.

Retention periods will be set, using the following criteria:

- The length of time the data needs to be retained to meet the identified purpose.
- Whether data needs to be retained to defend possible future legal claims.
- Legal or regulatory requirements.
- Industry standards or guidelines, such as the NHS' retention timescales.

6.1.6 Security, integrity and confidentiality

The cybersecurity measures we have in place and our organisational approach to data and IT security, is detailed in our Data and IT Security policy.

Security measures must cover every aspect of data processing and not just the way data is stored and transmitted (cybersecurity). As such, measures should ensure that:

- Data can only be accessed, amended, disclosed or deleted by those that have the authority to do so.
- Data is up to date, accurate and complete.
- Data continues to be accessible and usable, even if it is accidentally lost or damaged.

The level of security required is determined by what is appropriate given the data we process and the risks this presents to the organisation. The ICO details 2 categories of measures which

organisations should consider, to ensure data remains secure. These categories, along with the measures we have in place, are included below.

Organisational measures:

- Business continuity arrangements: Each business area has a business continuity plan which details the arrangements, should there be any interruption to service delivery.
- NHS Data Security and Protection toolkit: The DPO completes the toolkit for each business area which processes NHS data. This gives assurance that the organisation is adhering to the most current data protection and governance requirements.
- Audits, training, policies and guidance (see section 6.2)

Technical measures:

- Physical security: We have policies in place relating to the disposal of data (whether this has been stored electronically or on paper (see the Data and IT Security policy)) and relating to how devices should be kept secure. Each business area has a number of physical security measures, some of these may include:
    - CCTV
    - Access controlled doors
    - Alarms
    - Visitor signing in processes
- System, data, online and device security: The requirements in relation to each of these are detailed in our Data and IT Security policy. The requirements relating to personal devices, used for work purposes are detailed in our BYOD policy.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

Team members are responsible for protecting the personal data we hold. They must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. They must exercise particular care in protecting special categories of personal data and criminal convictions data from loss and unauthorised access, use or disclosure.

Team members must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Team members must not transfer personal data to third-party service providers unless this has been approved by the DPO.

Team members must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
- Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

- Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

6.1.7 Transfer limitation

The UK GDPR restricts the transfer of all personal data outside of the UK. This ensures that the level of data protection afforded to UK data, is not undermined by the transfer. A restricted transfer is taking place if the UK GDPR applies to the processing of the personal data we are wishing to transfer out of the UK. Transfers of data outside of the UK must not take place without the prior authorisation of the DPO.

Before making a restricted transfer, it should be determined whether the same result can be achieved, without actually transferring the data. If this is not possible, a restricted transfer can still take place in line with the GDPR, providing at least one of the following criteria apply. These must be assessed in the order they appear. If none of the criteria apply, then the transfer would be a breach of the UK GDPR.

1. Would the restricted transfer be covered by 'adequacy regulations'?

UK 'adequacy regulations' confirm that the legal framework in that country, adequately protects personal data and the rights of data subjects. Following the UK's departure from the European Union (EU) on 31 December 2020, existing EU adequacy decisions, are included as UK 'adequacy regulations'. For a list of the most current 'adequacy regulations', please visit the 'International transfers' section of the ICO's Guide to the UK GDPR.

2. Is the restricted transfer covered by appropriate safeguards?

A list of appropriate safeguards is included in the UK GDPR. Each of these ensures that both we, and the receiver of the personal data, is legally bound to protecting data subjects' rights and freedoms. The prescribed appropriate safeguards are:

i. A legally binding and enforceable instrument between public authorities or bodies.
ii. UK Binding Corporate Rules ('UK BCRs'): UK BCRs are intended for use by multinational corporate groups who are engaged in a joint economic activity. Previous EU BCR's have been incorporated into the UK GDPR. The ICO will now begin approving new BCRs.
iii. Standard contract clauses (SCCs): SCCs contain contractual responsibilities for both the sender and receiver of personal data, and rights for the data subjects whose personal data is transferred. Data subjects can directly enforce those rights against the sender or receiver of personal data. EU SCCs can continue to be used until the ICO has published UK SCCs. The EU SCCs can be altered so that they make sense in a UK context, but no other changes should be made.
iv. An approved code of conduct. Please note that there are no approved codes of conduct currently.
v. Certification under an approved scheme. Please note that there are no approved certification schemes currently.
vi. Contractual clauses authorised by the ICO: This is where a bespoke contract has been approved by the ICO.
vii. Administrative arrangements between public authorities or bodies: This is for use by

public bodies when they have a documented administrative arrangement in place which sets out appropriate safeguards and has been approved by the ICO.

If a proposed restricted transfer is covered by an exception, the transfer may go ahead. The 8 exceptions are:

- The data subject has given their explicit consent to the restricted transfer.
- The transfer is necessary to perform a contract with an individual.
- The transfer is necessary to enter into a contract with an individual that benefits another individual whose data is being transferred.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary in response to, to make or defend a legal claim.
- The transfer is necessary to protect the vital interests of a data subject, who is physical or legally unable to consent to the transfer.
- The transfer is a public register.

Before relying on an appropriate safeguard, we must conduct a risk assessment to ensure we are satisfied that the transferred data will continue to have a level of protection equivalent to the UK GDPR.

6.1.8 Data subject's rights and requests

The rights of data subjects and how we should respond to requests invoking these rights, is detailed in our Individual Rights and Data Access policy and procedure. However, in short, data subjects have the following rights in relation to their personal data:

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

Data subjects can also:

- Where consent is the lawful basis for processing, withdraw their consent at any time without fear of ill-treatment or recrimination.
- Prevent our use of their personal data for direct marketing purposes.
- Expect to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
- Make a complaint to the ICO.

The DPO must be informed of any requests, from data subject, to invoke any of their rights. The DPO should be informed as soon as the request is received.

6.2 Accountability and governance

Article 5(2) of the UK GDPR states: '*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*.' This requires data controllers to not only be responsible for compliance, but also requires them to demonstrate their compliance. As an organisation, we also want to demonstrate our compliance to data subjects, who have trusted us with their personal data.

We have adequate resources and controls in place to ensure and to document GDPR compliance including:

- Having a suitably qualified DPO (Nick Banister-Dudley, Head of Compliance) and an executive accountable for data privacy (Julie Rayner, Care Quality, Governance and Compliance Director and the Senior Information Risk Owner).
- Ensuring data protection activities are recorded appropriately and that we have appropriate policies and guidance in place (see section 6.2.1).
- Training (see section 6.2.2).
- Audit (see section 6.2.2).
- Implementing privacy by design approach (see section 6.2.3).

6.2.1 Record keeping

The GDPR requires us to keep full and accurate records of all our data processing activities. We must keep and maintain accurate corporate records detailing our data processing, consents given by data subjects' consents, subject access requests and personal data breaches.

These records will include, as a minimum, the name and contact details of the controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

We will also integrate data protection into internal documents including this policy, related policies, privacy guidelines and privacy notices. Policies are developed based on key data protection areas and are readily available to all team members, via the e-learning portal. Training on new policies is given, when required and appropriate.

Records are also kept in respect of:

- CCTV disclosures
- Legitimate interest assessments conducted
- Reviews of the record of processing
- Changes to the record of processing
- Data protection/privacy impact assessments conducted
- Data processing agreements
- Freedom of Information Act requests
- Other record requests
- Registration with, and fees paid to, the Information Commissioner's Office

6.2.2 Training and audit

The GDPR/data protection training requirements are detailed in section 7 of this policy. Training is delivered following the completion of an annual training needs analysis, conducted by the DPO and ratified by the Senior Information Risk Owner. Any training attended by team members, will be recorded.

We will also regularly test the privacy measures implemented, by conducting an annual audit to assess compliance. The outcome of these audits will be acted on to ensure the necessary improvements are made.

6.2.3 Privacy by design

We recognise that data protection by design and default is an integral element of being accountable. As such, we will embed data protection throughout our business operation. Teams will include the DPO in discussions regarding new, or amended, processing activities as detailed in section 6.1.1 of this policy.

The completion of a data privacy/protection impact assessment (DPIA) is a legal requirement where processing presents a high risk to rights and freedoms of data subjects. Team members are responsible for notifying the DPO prior to the introduction or commencement of:

- a major system or business change programme,
- new technologies (programs, systems or processes), or changing technologies (programs, systems or processes),
- automated processing including profiling and automated decision making,
- new large-scale processing of special categories of personal data or criminal convictions data, and
- large-scale, systematic monitoring of a publicly accessible area.

The DPO has the responsibility for conducting DPIAs, which will include:

- A description of the nature, scope, context and purposes of the processing.
- An assessment of the necessity and proportionality of the processing in relation to its purpose.
- An assessment of the risk to individuals.
- The risk mitigation measures in place and demonstration of compliance.

If, as part of the DPIA process, high risks are identified which cannot be mitigated, the ICO must be consulted before the processing takes place.

6.2.4 Data processing agreements

Data controllers are required to have a written contract in place with each data processor. Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the UK GDPR. Where service contracts do not contain the required information, a data processing agreement will be signed

by both parties. The internal relationship lead is responsible for ensuring that the necessary contract or agreement is in place, for each data processor they are responsible for.

6.2.5 Recording and reporting personal data breaches

The organisational expectations in relation to how team members should respond to personal data breaches, is detailed in our Personal data breach policy. However, in short, the Information Commissioner's Office (ICO) defines a personal data breach as a '*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.*'

If you are made aware of/suspect that a breach has occurred, all team members must immediately notify the DPO. The DPO can be contact by email on dpo@hallmarkcarehomes.co.uk.

6.3 Direct marketing

Most of the rules in The Privacy and Electronic Communications Regulations (PECR) apply to unsolicited marketing messages. PECR cover marketing by phone, fax, email, text or any other type of electronic mail. An unsolicited message is that which has not been specifically requested. As such, even if someone has 'opted in' to receiving marketing material from us, it still counts as unsolicited marketing. An opt-in means that the data subject agrees to future messages (and is likely to mean that the marketing complies with PECR). This does not make all unsolicited marketing unlawful. Unsolicited marketing messages can still be sent, as long as they comply with PECR. Solicited marketing messages are those which have been actively requested by a data subject.

A data subject's prior consent is required for direct marketing. The limited exception for existing customers known as 'soft opt-in', allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing ('opt out') must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information. A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

The rules on consent, the soft opt-in and the right to opt out do not apply to electronic marketing messages sent to businesses (B2B marketing). However, we must identify ourselves and provide our contact details, as well as making checks against the relevant preference service list, before contacting businesses.

6.4 Sharing personal data

Data sharing usually means disclosing personal data to third parties outside of the organisation.

We will only share the personal data we hold with third parties, such as our service providers, if all of the following apply:

- They have a need to know the information for the purposes of providing the contracted services.
- Sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained.
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place, evidence through a valid contract or data processing agreement.
- The transfer complies with any applicable cross-border transfer restrictions.
- The DPO has authorised the sharing.

Data may also need to be shared with organisations when we have a legal obligation to do so. Confidential health and social care data may also need to be disclosed and shared in line with the Caldicott Principles (1997) (see the Records Management and Retention policy).

6.5 Consent

As mentioned in section 6.1.1, consent is one of the lawful bases for processing personal data. Whilst we have Consent for inclusion in marketing activities policies (for residents, team members and external stakeholders), this section provides guidance on consent more generally.

Consent is defined in Article 4(11) of the UK GDPR as: "*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*". In short, the criteria for valid consent are thus:

- It must be freely given – this means data subjects should have a genuine choice over whether to give their consent to a type of processing, or not.
- It must be specified and informed – this means data subjects should be aware of the identity of the data controller, the purpose of the processing (including separate, granular consent for different processing operations).
- It must be given by an unambiguous indication - it must be obvious that the data subject has consented and what they have consented to. This requires more than just a confirmation that they have read terms and conditions – there must be a clear signal that they agree.

There may be times where explicit consent must be given. Consent that is inferred from someone's actions cannot be explicit consent, however obvious it might be that they consent. Explicit consent must be expressly confirmed in words (either orally or in writing).

Consent is seen to degrade over time, but how long it lasts will depend on the context in which

it was given. Consent cannot be implied, or bundled together, with other terms and conditions. As such, consent forms must be given separately and distinctly from other documents. Data subjects should also be given time to read and understand consent paperwork/forms.

We should also bear in mind that consent is more difficult to obtain where there is an imbalance of power e.g., between an employer and an employee. As such, data subjects can refuse to give, or withdraw consent, without any detriment or ill-treatment. We will take reports contrary to this, very seriously and these may be dealt with in line with our Disciplinary/Grievance procedures.

Article 7(1) of the UK GDPR requires data controllers to record the consent given by data subjects. Good records should include who consented, when they consented, the information the data subject(s) was given at the time, how the data subject consented and whether they have withdrawn consent.

Using consent as a lawful basis, must first be approved by the DPO. The DPO will ensure that the correct consent paperwork and privacy information has been created, prior to the start of the processing.

7. TRAINING AND OTHER RESOURCE IMPLICATIONS

Team members who regular handle personal data, including relevant Central Support team members and General Managers, will all receive face to face training in the application of policies and procedures linked to UK GDPR. This training will be refreshed at on an annual basis. Additional face to face training (for new team members who require this level of training) will be provided by the DPO.

Other team members who do not receive the initial face to face training, will receive GDPR training via an e-learning platform.

GDPR training (regardless of delivery) will be mandatory and will refreshed on an annual basis. All new team members will read the policies on data protection and on confidentiality as part of their induction process.

Senior team members will monitor the application of this policy via audit and observation.

Failure to adhere to the process as defined in this policy will be addressed via supervision or performance management processes.