Appropriate Policy Document

Version number	4.0
Date of issue	30/03/2022
Date for review	29/03/2023
Author	Head of Compliance & Data Protection Officer
Ratified by	Care Quality, Governance and Compliance Director & Senior Information Risk Owner
If you have any questions or concerns regarding the content of this document, please email Nick Banister-Dudley, Data Protection Officer on dpo@hallmarkcarehomes.co.uk.	

1. INTRODUCTION

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category and criminal offence data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1, Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require us to have an APD in place. (in line with Schedule 1 paragraphs 1(1)(b) and 5).

This document demonstrates that the processing of special category and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the UK General Data Protection Regulation (UK GDPR) Article 5 principles. It also outlines our retention policies with respect to this data.

1.1 Special category data

Article 9 of the UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

1.2 Criminal offence data

Article 10 of the UK GDPR applies to personal data relating to criminal convictions and offences. To process criminal offence data, organisations must either:

- process the data in an official capacity; or
- meet a specific condition in Schedule 1 of the Data Protection Act 2018 and comply with the additional safeguards set out in that Act.

2. DESCRIPTION OF THE DATA PROCESSED

Hallmark Care Homes processes special category data relating to:

- Care home visitors
- Enquirers
- External contractors and suppliers
- Prospective team members
- Residents
- Team members including contractors

- Volunteers

We also process criminal offence data regarding our team members, internal and external contractors, and volunteers.

As required by Article 30 of the UK GDPR, Hallmark Care Homes maintains a record of our processing activities. This is reviewed annually as a minimum, or sooner if we have changed our processing activities.

Data subjects are informed of our processing activities via privacy notices/policies:

- The Privacy Notice for current team members can be accessed via the e-learning portal and the policies page of our website.
- The Privacy Policy for all other data subjects (prospective team members, residents, relatives, supporters, friends, suppliers, website visitors and enquirers), can be accessed via the policies page of our website.

2.1 Care home visitors

Due to the ongoing COVID-19 outbreak, we will take visitors' (including relatives and other care home visitors e.g. external contractors) temperatures and health information (in respect of COVID-19 test results, exposure and symptoms). We will also process data relating to any injury sustained on our premises in line with legal requirements.

2.2 Enquirers

We process health data regarding enquirers, if they are also prospective clients. This is processed in line with health and social care legislation in England and Wales, so that we can determine whether our care services can meet your needs.

2.3 External contractors and suppliers

In order to meet the relevant health and social care legislation, we request copies of external contractors' and suppliers' Disclosure and Barring Service (DBS) checks. These are only requested from external contractors or suppliers that conduct unsupervised work in one of the homes, to ensure resident safety.

2.4 Prospective team members

We process the special category data about our prospective team members that is necessary to fulfil our legal and contractual obligations as an employer/business. Each prospective team member completes a medical questionnaire, which helps us assess the support we need to offer in terms of their health or disabilities. Information on race and ethnicity is collected to monitor diversity within the organisation. We also collect data relating to a team member's right to work in the UK, in order to meet the relevant legislation.

In order to meet the relevant health and social care legislation, we conduct Disclosure and Barring Service (DBS) checks to get details on any criminal convictions.

2.5 Residents

Residents living in one of our care homes receive personal or nursing care. Both of these are activities regulated by the Care Quality Commission (CQC) in England and Care Inspectorate Wales (CIW) in Wales. In order to provide these services, in line with regulatory requirements, we process health and medical data. This includes processing health data about health interventions and treatments. This data may be shared with regulatory bodies such as the CQC, CIW, safeguarding teams and local authorities, as well as other health and social care professionals. We will also process data relating to any injury sustained on our premises in line with legal requirements.

We also process health data to maintain oversight of business operations and for the purposes of due diligence, as well as to maintain contracts with residents and the relevant funding authorities.

In response to the ongoing COVID-19 pandemic, in line with Government guidance, we conduct regular COVID-19 tests and process the details and results of these.

2.6 Team members (including contractors)

We process the special category data about our team members, contractors and volunteers that is necessary to fulfil our legal and contractual obligations as an employer/business. Each team member completes a medical questionnaire, which helps us assess the support we need to offer in terms of their health or disabilities. Health information is also retained to meet our legal obligations in respect of team member's fitness to return to work after absence due to sickness, as well as entitlement to state benefits. Information on race, ethnicity and sexual orientation is collected to monitor diversity within the organisation. We also collect data relating to a team member's right to work in the UK, in order to meet the relevant legislation. We share this data with relevant government departments and regulators, as well as insurers and legal professionals.

We will also process data relating to any injury sustained on our premises in line with legal requirements. We share this data with relevant government departments and regulators, as well as insurers and legal professionals.

We also process health data to maintain oversight of business operations and for the purposes of due diligence

We also collect details of whether a team member belongs to a trade union. This is only shared with us, by team members, as part of formal human resource processes.

Due to the ongoing COVID-19 panedmic, we are also processing further health data concerning team members i.e. the details and result of their COVID-19 test. We also process team members' (temperatures and health information (in respect of COVID-19 exposure and symptoms).

In order to meet the relevant health and social care legislation, we conduct Disclosure and Barring Service (DBS) checks to get details on any criminal convictions.

2.7 Volunteers

Each volunteer completes a medical questionnaire, which helps us assess the support we need to offer in terms of their health or disabilities.

Due to the ongoing COVID-19 pandemic, we also process further health data concerning volunteers i.e. the details and result of their COVID-19 test. We also process volunteers' (temperatures and health information (in respect of COVID-19 exposure and symptoms).

3. PROCEDURES FOR ENSURING COMPLIANCE WITH THE PRINCIPLES

The points below briefly explain how Hallmark Care Homes processes special category and criminal offence data in compliance with the principles of the UK GDPR.

3.1 Accountability principle

As required by the UK GDPR and DPA 2018, the Hallmark Care Homes group of companies have a Data Protection Officer (DPO). The DPO is registered with the Information Commissioner's Office (ICO).

The DPO highlights any key data protection risks at the quarterly Risk Management Group meeting. The DPO submits a detailed report to this Group, quarterly.

We also complete the NHS Data Security and Protection Toolkit self-assessment annually, for each care home.

3.1.1 Do we maintain appropriate documentation of our processing activities?

A record of processing is maintained and updated when there are changes to our processing activities. The relevant privacy notices are then changed in light of this. In addition to this, we also maintain a number of data protection logs:

- Legitimate interest assessment log
- A log recording changes to the record of processing
- Record of decisions log
- Data privacy impact assessment log
- Data processing agreement log
- Freedom of Information request log
- Record request log
- Personal data breach log
- Subject access request log

3.1.2 Do we have appropriate data protection policies?

We have a number of data protection policies:

- Bring your own device (BYOD) policy
- CCTV policy
- Central Support (Head Office) office security policy
- Consent for inclusion in marketing activities policies (for residents, team members and external stakeholders)
- Data and IT security policy
- Data protection/GDPR policy
- External storage and archiving policy
- Individual rights and data access policy
- Personal data breach policy
- Records management and retention policy

All are reviewed every 3 years, or sooner, if there is a change in legislation or best practice. Policies are developed by the DPO and ratified by the Senior Information Risk Owner. This role is held by the organisation's Care Quality, Governance and Compliance Director.

3.1.3 Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?

Data controllers must conduct DPIAs ahead of high-risk processing. This requirement is detailed in our Data protection/GDPR policy. A DPIA will be conducted when we are implementing major system or business change programs involving the processing of personal data including:

- The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes).
- Automated processing including profiling and automatic decision making.
- Large-scale processing of special categories of personal data or criminal convictions data.
- Large-scale, systematic monitoring of a publicly accessible area.

Our DPIAs will include:

- A description of the processing, its purposes and our legitimate interests, if appropriate.
- 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.

3.1.4 Technical and organisational measures in place to protect data.

We have a number of technical and organisational measures in place to protect all data, including special category and criminal offence data. These are:

- A suite of data protection policies which detail company expectations on the processing, management and security of personal data. See section 3.1 for more information.
- Physical access security to buildings, rooms and cabinets containing personal data in the

form of codes or locks.
- Password requirements for network and systems access.
- Email encryption system to ensure email communications containing personal data are secure.
- Antivirus and malware systems
- Annual GDPR audit of each home to assess their adherence to prescribed policies.
- Annual training (either e-learning or face to face) which provides information to team members on how to handle data securely.

3.2 Principle (a): lawfulness, fairness and transparency

We have identified an appropriate lawful basis, and a further Schedule 1 condition, for processing special category and criminal offence data. These are detailed in section 5 of this document.

We make appropriate privacy information available with respect to the special category and criminal offence data we process:

- Privacy and fair processing notice for current team members is available on the e-learning portal and the policies page of our website.
- Privacy and fair processing notice for prospective team members is available on our website here.
- The Privacy policy for residents, relatives, suppliers, website/social media visitors and enquiries, is available on our website here.

These notices/policies provide accurate information on when we collect the special category or criminal offence data. They detail why this data is needed and the rights that data subjects have in relation to this.

3.3 Principle (b): purpose limitation

We have clearly identified our purpose(s) for processing special category and criminal offence data. We have included appropriate details of these purposes in our privacy information for data subjects.

If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), we will check that this is compatible with our original purpose or get specific consent for the new purpose.

3.4 Principle (c): data minimisation

We only collect the special category or criminal offence data we actually need for our specified purposes. We have the sufficient amount of this data to ensure that we can properly fulfil the identified purposes.

3.5 Principle (d): accuracy

Data is reviewed regularly to ensure that it is still accurate, where relevant. The frequency of

this review depends on the data being processed. For example, care plan documentation is reviewed monthly and evaluated biannually (in England) or quarterly (in Wales), and criminal record checks are renewed every 3 years. Policies and procedures are in place which state the organisation's expectations with regards to maintaining the accuracy of data.

If data is inaccurate, data subjects can request that this is rectified. How data subjects can invoke their right to rectification is detailed in our Individual Rights and Data Access policy. A copy of which is available on our website here. Where data has been rectified, we will keep a record of the mistake and ensure lessons are learnt following this.

3.6 Principle (e): storage limitation

The special category and criminal offence data processed by us, is detailed in our record of processing and in our Records Management and Retention policy. Retention timescales are determined based on our legal obligations, as well as our interests and needs as a business. Where possible, we aim to mirror our retention timescales with those of NHS England.

Our Records Management and Retention policy also details how data should be archived and disposed of, when the retention timescale has passed. Spot checks of these processes are conducted by the DPO as part of their annual GDPR audit.

3.7 Principle (f): integrity and confidentiality (security)

We have appropriate policies, procedures, and technical and organisational measures, to protect electronic and hard copy information. These are reviewed regularly and assessed as part of the annual GDPR audit conducted by the DPO.

A DPIA will be conducted when we are implementing major system or business change programs, involving the processing of personal data. DPIAs include an assessment of the risks to individuals and the risk mitigation measures in place.

4. RETENTION AND ERASURE POLICIES

Our retention timescales are detail in our retention schedule, which is included in our Records Management and Retention policy and record of processing.

Special category data is retained for:

- Residents: 7 years after death or from moving out from one of our care homes. We hold data relating to non-serious accidents for 10 years and 20 years for serious accidents.
- Team members (including contractors and volunteers): 7 years after our employment contract, volunteer agreement or contractor agreement has ended. In respect of dermatitis risk assessments or annual skin surveillance, these are retained for 40 years from the date of the screening. We hold data relating to non-serious accidents for 10 years and 20 years for serious accidents.
- Prospective team members: Data will be held for 2 years if a prospective team member is unsuccessful in their application. If an offer of employment is made, this data will be retained for 7 years, as stated above for team members.

- Care home visitors (including external contractors and suppliers): 6 months following the official end of the COVID-19 outbreak. We hold data relating to non-serious accidents for 10 years and 20 years for serious accidents.

Criminal offence data retained for:

- Team members (including contractors and visitors): 7 years after our employment contract, volunteer agreement or contractor agreement has ended.
- Prospective team members: Data will be held for 2 years if a prospective team member is unsuccessful in their application. If an offer of employment is made, this data will be retained for 7 years, as stated above for team members.
- External contractors and suppliers: 1 month after the contract ends or for 3 years from the last time work was conducted for us (for contracts with no end date).

Hard copy data is either shredded or destroyed. IT equipment, potentially containing special category or criminal offence data, is destroyed securely.

5. SCHEDULE 1 CONDITIONS FOR PROCESSING

We can only process special category data if we can meet one of the specific conditions in Article 9 of the UK GDPR. Five of the conditions for processing are provided solely in Article 9 of the UK GDPR. The other five require authorisation or a basis in UK law, which means we need to meet additional conditions set out in the Data Protection Act (DPA) 2018.

Data	Who it relates to	Reason for processing	Lawful basis (Article 6)	Condition for processing (Article 9/Schedule 1)
Health data relating to physical and mental health	Care home visitors	Accident and incident management	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health: COVID test details and result	Care home visitors	COVID-19 risk mitigation	6(1)(e): we are carrying out tasks in the public interest	Article 9(2)(i) - public health [DPA 2018, Schedule 1, Part 1, paragraph 3]
Health data relating to physical and mental health	Care home visitors	COVID-19 risk mitigation	6(1)(e): we are carrying out tasks in the public interest	Article 9(2)(i) - public health [DPA 2018, Schedule 1, Part 1, paragraph 3]
Health data relating to physical and mental health	Enquirers	Enquiry management	6(1)(f): it's in our legitimate interests	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Criminal convictions	External contractors	Legal and regulatory compliance	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health data relating to physical and mental health	Prospective team members	Recruitment	6(1)(b): steps are required prior to a contract with the data subject	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care

Data	Who it relates to	Reason for processing	Lawful basis (Article 6)	Condition for processing (Article 9/Schedule 1)
				systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Criminal convictions	Prospective team members	Recruitment	6(1)(b): steps are required prior to a contract with the data subject	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Racial or ethnic origin	Prospective team members	Recruitment	6(1)(b): steps are required prior to a contract with the data subject	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]
Health data relating to physical and mental health	Residents	Accident and incident management	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health data relating to physical and mental health	Residents	Business operations and due diligence	6(1)(f): it's in our legitimate interests	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health data relating to physical and mental health	Residents	Contract management	6(1)(b): we have a contract with the data subject	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]
Health: COVID test details and result	Residents	COVID-19 risk mitigation	6(1)(e): we are carrying out tasks in the public interest	Article 9(2)(i) - public health [DPA 2018, Schedule 1, Part 1, paragraph 3]
Health data relating to physical and mental health	Residents	Delivery of health and social care	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]

Data	Who it relates to	Reason for processing	Lawful basis (Article 6)	Condition for processing (Article 9/Schedule 1)
Data regarding religious or philosophical beliefs	Residents	Delivery of health and social care	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Data regarding sexual orientation	Residents	Delivery of health and social care	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health data relating to physical and mental health	Residents	Health data sharing with GP services (at Kew House only)	6(1)(e): we are carrying out tasks in the public interest	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health: COVID test details and result	Residents	Legal and regulatory compliance	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health data relating to physical and mental health	Residents	Legal and regulatory compliance	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health data relating to physical and mental health	Team members	Accident and incident management	6(1)(c): we have to comply with a legal obligation	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]
Health data relating to physical and mental health	Team members	Business operations and due diligence	6(1)(f): it's in our legitimate interests	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]

Data	Who it relates to	Reason for processing	Lawful basis (Article 6)	Condition for processing (Article 9/Schedule 1)
Health: COVID test details and result	Team members	COVID-19 risk mitigation	6(1)(e): we are carrying out tasks in the public interest	Article 9(2)(i) - public health [DPA 2018, Schedule 1, Part 1, paragraph 3]
Health data relating to physical and mental health	Team members	COVID-19 risk mitigation	6(1)(e): we are carrying out tasks in the public interest	Article 9(2)(i) - public health [DPA 2018, Schedule 1, Part 1, paragraph 3]
Health data relating to physical and mental health	Team members	Employee performance management	6(1)(c): we have to comply with a legal obligation	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]
Trade union membership	Team members	Employee performance management	6(1)(c): we have to comply with a legal obligation	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]
Criminal convictions	Team members	Employment	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health data relating to physical and mental health	Team members	Employment	6(1)(c): we have to comply with a legal obligation	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]
Racial or ethnic origin	Team members	Employment	6(1)(c): we have to comply with a legal obligation	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]
Data regarding sexual orientation	Team members	Employment	6(1)(c): we have to comply with a legal obligation	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]
Health data relating to physical and mental health	Team members	Health and safety	6(1)(c): we have to comply with a legal obligation	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]
Health data relating to physical and mental health	Team members	Legal and regulatory compliance	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care

Data	Who it relates to	Reason for processing	Lawful basis (Article 6)	Condition for processing (Article 9/Schedule 1)
				systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health data relating to physical and mental health	Team members	Legal and regulatory compliance	6(1)(c): we have to comply with a legal obligation	Article 9(2)(i) - public health [DPA 2018, Schedule 1, Part 1, paragraph 3]
Health data relating to vaccinations	Team members	Management of infectious illnesses	6(1)(f): it's in our legitimate interests	Article 9(2)(i) - public health [DPA 2018, Schedule 1, Part 1, paragraph 3]
Criminal convictions	Volunteers	Volunteer recruitment and ongoing volunteering	6(1)(c): we have to comply with a legal obligation	Article 9(2)(h) - provision of health or social care or treatment or the management of health or social care systems and services [DPA 2018, Schedule 1, Part 1, paragraph 2]
Health: COVID test details and result	Volunteers	Volunteer recruitment and ongoing volunteering	6(1)(c): we have to comply with a legal obligation	Article 9(2)(i) - public health [DPA 2018, Schedule 1, Part 1, paragraph 3]
Health data relating to physical and mental health	Volunteers	Volunteer recruitment and ongoing volunteering	6(1)(c): we have to comply with a legal obligation	Article 9(2)(b) - Employment, social security and social protection [DPA 2018, Schedule 1, Part 1, paragraph 1]