DATA PROTECTION IMPLEMENTATION POLICY – MAY 2018

INTRODUCTION

St Philips recognises the importance of managing personal data in a responsible and appropriate manner. In particular, the organisation has reviewed its data protection policy in light of the General Data Protection Regulation (EU) 2016/679 ("GDPR"). We will seek to observe the 6 principles set out in the GDPR. We set out below our practice and procedures to be followed by all St Philips Care employees or contractors in future. If you have any questions or concerns about the Policy or any matters relating to personal data, you should refer these to the Data Protection Officer (DPO).

Policy	**Procedure**
1. To process personal data lawfully using the legal bases set out in the GDPR (Principle 1).	1.1. Ensure that we have resident, employee or individual third party consent to use their personal information, or have a legitimate interest in using that information. Wherever possible, we will tell these parties why we need their personal information. 1.2. This will usually be in our privacy notice, the resident service user agreement terms and conditions and employee handbook so it is important that signed copies are provided by each resident or employee, as appropriate, and kept on file.
2. To operate technical and organisational security measures to ensure the security of personal data (Principle 6).	2.1. Building security. Most of our homes are locked to prevent unauthorised access. Where a keyphone entry system is in operation, access codes may only be given to staff, permitted contractors and residents' families. If you suspect or discover that an unauthorised person knows the access code, notify the manager to arrange the changing of the code and informing of all relevant parties. In our Mental Health homes, some homes operate an open door policy but the duty team are responsible for monitoring access points and external access points (for example, driveways) to the premises.

	2.2. All staff must be aware of the need to exclude uninvited persons from our premises. Ensure doors are locked , do not allow “tailgating” by strangers, be prepared to politely challenge strangers to check that they are entitled to be in the building. 2.3. IT security. We must protect information and data from all threats, whether internal, external, deliberate or accidental and guard that information from unauthorised access. We safeguard the integrity of information we hold. Wifi codes should be controlled to prevent unauthorised parties getting access. 2.4. PCs and laptops. All PCs and laptops (and any other devices containing personal information) must be password protected using a secure, memorable password. Change passwords frequently, particularly if you suspect someone has become aware of yours without permission. Staff should use your own log in if you have one. All staff must log off when you have finished using a PC or laptop. 2.5. Maintain good general housekeeping. St Philips Care acknowledges that we hold sensitive personal data about our residents (eg MAR sheets, care plans, care records) and must pay particular attention to keeping this extremely personal information safe. 2.6. Some work stations are in accessible places (eg corridors). Wherever you work, put files with sensitive personal information (for example care plans, medical records, bank details or employee data) away after use. Avoid leaving loose papers or files containing personal information on work areas or accessible to strangers (eg visitors or

	cleaners). If you have a lockable desk or drawer, or filing cabinet, lock it when you are away from it and only give access to staff who need to share those files. 2.7. If you use noticeboards setting out personal information about residents, control access by visitors and cover these noticeboards if third parties are in the room. 2.8. Transport of paper files etc. When out of the office take proper precautions to keep these safe and secure. Do not leave them unattended if possible. If travelling by car, keep files out of public sight and locked in the boot when you are no longer in your vehicle. 2.9. Residents may travel to hospital or doctors' surgeries and other venues for treatment. Any accompanying party should be asked to securely keep the PCS records or other personal details if the resident is not able to do so. If the local health authority uses red bags for the carrying of medical data, please use them. 2.10. Only Company issued USB sticks may be used. These are encrypted for greater security. CDs, floppy disks should never be used to store personal data. 2.11. Emails. Always check the recipient is the person you want to send to and don't copy it to other parties without checking they need to see it or the subject has given permission. Do not allow access to your emails to other members of staff who have no need to read your emails or see confidential or personal data about others. Do consider encryption or password protection of zipped files attached to emails for sensitive personal data sent by email.

	2.12. Post. Again always check the recipient and address details are correct. If you are opening the post, please do so in a secure location away from third parties. If you are sending confidential information from a home to head office, use recorded delivery or signed for post. 2.13. Fax. If you send a fax, contact the receiving party and advise them that you are sending personal information by fax and ask them to retrieve the material from their fax machine upon receipt.
3. Document storage, retrieval and destruction (Principle 5).	3.1. We recognise that the GDPR encourages every organisation to minimise the amount of personal data we obtain, tell people how long we will keep it and destroy it promptly and securely. Our policy is essentially to hold files for 7 years from date of closing. 3.2. Before destruction of records, files must be securely stored in the archive room or at an off-site, secure location. Access to old records must be restricted to staff that are required to have sight of these. 3.3. Staff must conduct an annual review of the schedule of historic records and arrange secure destruction of files over 7 years' old. 3.4. We have special arrangments for storing employee and residents' information for safeguarding purposes as set out in our Safeguarding Policy and Staff Handbook.

4. To conduct marketing activity based on legitimate interests where appropriate, otherwise only to parties who have given their consent to receive marketing materials etc (Principle 2).	4.1. Given the nature of our marketing activity at St Philips Care, we believe that our activities comply with GDPR. 4.2. We do not contact individuals and market direct. We understand that word of mouth, direct approaches to a home and contacts through Social Services are appropriate and compatible with data protection principles. 4.3. Use of SOPs and SUGs is acceptable.
5. Not to capture personal data through our website (Principle 2).	5.1. News sections may contain personal data and where we use images, we will seek consent from the parties involved. 5.2. The 'Contact Us' form requires a person to enter their own details for contact to be made by us and sends an emails to enquiries@stphilipscare.com for us to respond outside of the website. 5.3. Any content resulting in an application being made through the St Philips Care website will need to be completed by the applicant and submitted through Indeed. No personal data will be captured by the website for job applications. Application forms and CVs will be destroyed within 12 months (save in relation to a successful job applicant). 5.4. We will review the website privacy statement annually each May.
6. To review our supply contracts and monitor for GDPR compliance (Principle 4).	6.1. Ensure that for new contracts or renewals of contracts where we provide or receive personal data, the responsibilities of each party are clearly identified. The risks and responsibilities arising through GDPR should be considered and allocated appropriately, with necessary reporting and penalties around potential breaches.

7. To respond to subject access requests within 30 days of receipt of a bona fide request.	7.1. Any request that appears to be a subject access request is to be referred to the Data Protection Officer and Managing Director as soon as practicable after receipt (with a copy to Head of Care). 7.2. The Data Protection Officer and Head of Care to consider the request, check that it is a subject access request under GDPR and prepare a response within 21 days. 7.3. Managing Director or their nominee is to approve the response within 7 days and authorise the despatch.
8. To respond to a request for rectification or erasure of personal data without undue delay.	8.1. Where an individual requests us to correct inaccurate personal data about him or her, this should be considered and acted upon promptly.(Examples include a name, address, email, telephone number). 8.2. Where an individual requests us to delete or destroy (erase) their personal data, a written copy of the request should be forwarded to the Managing Director and copied to the Head of Care for action. We have legal obligations why it may not be possible or practicable to comply with such a request.
9. To notify the Information Commissioner's Office (ICO) of any personal data breach as required by GDPR.	9.1. Ensure all staff are aware of the need to refer loss of personal data to ICO. 9.2. Potential notifications should be referred to care home managers or heads of department at head office within 24 hours of staff becoming aware of a data loss. 9.3. Managers or heads of department must determine within a further 24 hours whether the incident requires notification and report in writing either way to the

	Managing Director. 9.4. Managing Director may override the recommendation of a manager or head of department and submit a notice or not but if a notice is required, it must be submitted within 72 hours or provide reasons for the delay. 9.5. Guidance on what to report or not will be produced and reviewed/updated regularly by the Data Protection Officer in line with experience and direction from ICO. 9.6. Written reports of all data breaches (whether notified or not) will be kept in a central register at head office. 9.7. In exceptional cases, where the breach presents a high risk, it will be necessary to advise the data subject (eg resident or employee) in plain language and without delay. This communication must be approved in advance by the Managing Director.
10. To train our staff to be aware of the Policy and GDPR.	10.1. Issue a copy of this Policy to all staff and contractors and ensure they acknowledge receipt and that they have read the Policy. 10.2. Carry out regular training on the new data protection legislation for all members of staff. 10.3. Make sure that new employees or contractors are made aware of the Policy as part of their induction. 10.4. Circulate any revisions to this Policy to staff.

11. To carry out data protection impact assessments (PIA) in appropriate cases.	11.1. Where the organisation is looking at new technology or high risk/high value activity involving the processing of individuals' data then the budget holder must notify the Managing Director and produce a privacy impact assessment for approval before proceeding. 11.2. We will keep copies of any PIA for 7 years.
12. Not to use personal data for any purposes associated with automated individual decision- making (or profiling).	12.1. Not to approve any proposal that might involve software or other systems capable of processing personal data for profiling or similar.
13. To maintain any necessary record of our processing activities.	13.1. One new requirement under GDPR is to maintain written records with the information set out in Article 30 of the GDPR. These may be subject to inspection by ICO at their request. Records at our homes and head office must be kept in good order and accessible for inspection.
14. To review this Policy annually.	14.1. The Managing Director is responsible for this Policy and for monitoring compliance. The Data Protection Officer is to undertake an annual review to verify it is in effective operation across the business.