Facility	**Trinity Care**
Document Title and Code:	**Data Protection and Records Management Policy (Include GDPR).**
Code:	**TC10**
Version:	**2**
Author:	**Nursing Matters – Diarmuid O'Reilly, Susan McLaverty**
Approved & Authorised by:	**Changes adapted for local use by Directors of Nursing, Gormanston Wood, St. Peters NH, Suncroft Lodge NH, St. Doolaghs Park Care and Rehabilitation Centre, Foxrock NH, Castlemannor NH, AnovoCare NH**
Version Date :	**December 2018**
Review date:	**November 2021**
Responsibility for Implementation by:	**Director of Nursing**

1.0 Policy Statement:

This policy aims to set out the process of receiving, maintaining, managing, storing and disposal in a confidential manner of staff and resident's personnel data.

2.0 Purpose:

2.1 To ensure that all staff employed by or contracted to the nursing home will be aware of legal and professional requirements for the management of private and personal health information related to residents and themselves.

2.2 To ensure that all staff and residents are aware of their legal right to access their personal information stored by the Home

3.0 Objectives:

3.1 To ensure that all staff are aware of the legal, ethical, and professional requirements for the management of their records and the residents' personal and healthcare records.

3.2 To ensure that each person's rights to privacy, information protection and confidentiality are maintained.

3.3 To ensure that all records containing personal and healthcare information are completed, maintained, stored and disposed of in accordance with legal and professional requirements.

4.0 Scope:

4.1 Persons to whom this policy applies

This policy applies to all staff employed in or contracted to St PetersHomes who are involved in the creation, processing, storage, maintenance and disposal of those categories of records outlined in **4.2** below.

4.2 **Categories of records governed by this policy**

This policy applies to:

1. Records that contain personal data of any individual.
2. Records stipulated in Schedules 2, 3 and 4 and 5 of the Health Act 2007 (Care and Welfare of residents in designated centres for older people) Regulations 2013. These are:

- Documents to be held in respect of the Person-in-charge and for each member of staff
- Records to be kept in a designated centre in respect of each resident
- The current Statement of Purpose
- The current Residents' Guide
- Copies of all inspection reports
- A record of the designated centre's charges to residents, including any extra amounts payable for additional services not covered by those charges, and the amounts paid by or in respect of each resident.
- Records of the food provided for residents in sufficient detail to enable any person inspecting the record to determine whether the diet is satisfactory in relation to nutrition and otherwise, and of any special diets prepared for individual residents.
- A record of all complaints made by residents or representatives/relatives of residents or by persons working at St Petersabout the operation of the designated centre, and the action taken by the Registered Provider in respect of any such complaint.
- Notifications under Regulation 31
- Records of each fire practice, drill or test of fire equipment (including fire alarm equipment) conducted in the designated centre and of any action taken to remedy any defects found in the fire equipment.
- Records of the number, type and maintenance record of fire-fighting equipment.
- A record of all visitors to the designated centre, including names of visitors.
- Policies and procedures
- Health and safety records
- Quality and audit records

5.0 Definitions:

5.1 **Data Subject**

A data subject refers to an identified or identified living person (GDPR). It is the individual the personal data relates to (Data Protection Commissioner, 2017). In the context of this policy, a data subject is any living person whose personal data is obtained and processed by Trinity Care. For example, residents, employees, residents' representatives or family members whose personal data is obtained and processed by Trinity Care.

5.2 **Personal Data**

Personal data means any identifiable information relating to a living individual ('data subject'). This means information by which the individual can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person (General Data Protection Regulation).

5.3 **Special categories of personal data**

Refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5.4 **Genetic Data**

'Genetic data' means *'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;'* (General data Protection Regulation).

5.5 **Biometric Data**

Biometric data' means '*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprints) data';* (General data Protection Regulation).

5.6 **Data Concerning Health**

'Data concerning health' means *'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;'* (General data Protection Regulation).

5.7 **Data Controllers**

A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files. Data controllers can be either individuals or "legal persons" such as companies, Government Departments and voluntary organisations. Examples of cases where the data controller is an individual include general practitioners, pharmacists, politicians and sole traders, where these individuals keep personal information about their patients, clients, constituents, etc. https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm. accessed 11/04/2018.

5.8 **Data Processor**

A data processor is a person who processes personal data on behalf of a data controller (General Data Protection Regulation) but does not include an employee of a data controller who processes such data during his/her employment. Individuals such as GPs, pharmacists or sole traders are considered to be legal entities. https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm. accessed 11/04/2018.

5.9 **Processing**

'Processing' means '*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,*

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction' (General Data Protection Regulation).

5.10 **Disclosure**

Disclosure refers to the release of personal data or personal information to a third party outside of the original specified purpose of obtaining the data/information. (Data Protection Commissioner, 2013).

5.11 **Privacy**

In terms of personal health information, privacy can be described as the right of individuals to keep their information confidential and is a human right enshrined in both Irish and European legislation. (HIQA, 2017).

5.12 **Third Party**

'Third party' means '*a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;* (General Data Protection Regulation).

5.13 **Consent**

'Consent' of the data subject means '*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'* (General Data Protection Regulation).

5.14 **Personal Data Breach**

Personal data breach' means '*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;'* (General Data Protection Regulation).

6.0 Legal and Professional Framework for Records Management

6.1 **Legal Basis for Processing Personal Data**

Under European and National Data Protection legislation, processing of personal data is lawful only *(referred to as the 'legal basis' for processing personal data)* if and to the extent **that at least one** of the following applies:

a) The data subject has given consent to processing his/her personal data for one or more specific purposes. This consent is subject to conditions outlined under.
b) The processing of the data is necessary for performance of a contract to which the person is party or to take steps at the request of the person prior to entering into a contract.
c) Processing is necessary for the controller to comply with a legal obligation.
d) Processing is necessary to protect the vital interests of the person or of another living person.
e) Processing is necessary for the performance of a task carried out in the public interest

or in the exercise of the official authority vested in the controller.

f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child.

In addition to the conditions outlined above, the processing of personal data is only lawful if it complies with the principles outlined in 6.5

(GDPR and Data Protection Act, 2018).

6.2 **Processing of special categories of personal data**

Special categories of personal data refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Processing of special categories of personal data is allowed only if it complies with the principles outlined in 6.5 **and one** of the following applies.

a) The data subject has given explicit consent to the processing of the special category of personal data for one or more specified purposes (Data protection Act 2018).

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social welfare law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (Data Protection Act 2018; General Data Protection Regulation).

c) 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; (General Data Protection Regulation) including to prevent injury or other damage to the data subject or another individual and to prevent loss, in respect of, or damage to property (Data Protection Act 2018).

d) Processing relates to personal data which are manifestly made public by the data subject; (General Data Protection Regulation).

e) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (General Data Protection Regulation) including for obtaining legal advice or in connection with legal claims, prospective legal claims, legal proceedings or prospective legal proceedings (Data Protection Act 2018).

f) Processing is necessary for medical purposes and is carried out by or under the responsibility of a health practitioner or a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that duty of confidentiality owed by a health practitioner.

g) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services based on Union or Member State law or pursuant to contract with a health professional and subject to the conditions of professional secrecy (General Data Protection Regulation).

h) Processing is necessary for reasons of public interest in public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures

to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

i) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6.3 **National Regulations for Designated Centres**

Under the Health Act 2007 (Care and Welfare of Residents in Designated Centres for Older People Regulations 2013), St Petersis obliged to create, maintain and retain a range of records related to carrying out of its business as a designated centre for older people. These records are listed in Schedules 2, 3 and 4 of the regulations and the obligations are outlined within the articles of the regulations.

6.4 **Additional Legislative Requirements**

In addition to data protection legislation, St Petershas additional record keeping obligations under employment law and health and safety legislation. These are:

- Organisation of Working Time Act 1997
- The Organisation of Working Time (Records) (Prescribed Form and Exemptions) Regulations 2001
- The Parental Leave Acts 1998 and 2006
- The Terms of Employment (Information) Act 1994
- The Safety, Health and Welfare at Work Act 2005
- The Safety, Health and Welfare at Work (General Applications) Regulations 1993)

6.5 **Principles relating to processing of personal data**

Under European and National legislation, St Petersis obliged to ensure that personal data is:

1. Obtained and processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Information is collected only for one or more specified, explicit and lawful purposes
3. Information is kept safe and secure
4. Information is kept accurate, complete and up-to-date
5. Information is adequate, relevant and not excessive
6. Information is retained for no longer than is necessary for the purpose or purposes and according to legal requirements.
7. The Controller shall be responsible for, and be able to demonstrate compliance with, the 6 points above. (Accountability)

6.6 **Professional Requirements**

Doctors, registered nurses and allied healthcare professionals are also obliged to comply with professional codes, standards and guidance related to residents' personal information. These include:

- Nursing and Midwifery Board of Ireland 2015 Recording Clinical Practice, guidance to Nurses & Midwives.
- Nursing and Midwifery Board of Ireland 2014 Code of Professional Conduct and Ethics for Nurses & Midwives.
- Medical Council of Ireland Guide to Professional Conduct and Ethics for Registered Medical Practitioners. 8th Edition, 2016.

7.0 Responsibilities

7.1 Responsibilities of the Registered Provider and Data Protection Lead of Trinity Care

The Registered Provider and Data Protection Lead of Trinity Care, have the following responsibilities regarding records management in Trinity Care:

7.1.1 Ensuring that all records as outlined in the Health Act, 2007 (care and welfare of residents in designated centres for older people) Regulations 2013 are kept in Trinity Care.

7.1.2 Ensuring that the creation, access to, maintenance, retention and destruction of records complies with legislative and regulatory requirements.

7.1.3 Ensuring that there are appropriate arrangements in place to facilitate compliance with legislation and professional requirements for management of personal data.

7.1.4 Ensuring that service level agreements are in place with any third-party contractor involved in the processing, storage or destruction of records, including arrangements for security and confidentiality of information.

7.1.5 Ensuring that arrangements are in place so that data subjects are given information about the purpose of collecting their personal data and how this information will be used.

7.1.6 Ensuring that arrangements are in place for safeguarding the confidentiality and privacy of all personal data.

7.1.7 Ensuring that information that may be required while providing care and services to residents is accessible to and easily retrieved by relevant staff.

7.1.8 Ensuring that St Petersmaintains a data register as outlined in this policy.

7.1.9 Ensuring that Data Privacy Impact Assessments are carried out in accordance with this policy.

7.1.10 Ensure that appropriate processes are in place to ensure any actual or suspected breach of personal data is investigated and notified in accordance with legislative requirements.

7.2 **Responsibilities of the Person in Charge**

7.2.1 Disseminating this policy to all staff and ensuring that staff have read and understand their responsibilities for records management and data protection in accordance with their roles.

7.2.2 Identifying any training needs for staff to implement this policy and ensuring staff have access to same.

7.2.3 Ensuring that this policy is reviewed at least 3 yearly or where there is any change in legislation, standards or practice affecting records management.

7.2.4 Ensuring that audits of healthcare records are carried out to ensure that these records are created and maintained in accordance with national standards, regulations and professional requirements.

7.2.5 Assisting with the creation and maintenance of the Data Register and any Data Privacy Impact Assessments required in accordance with the requirements outlined in this policy.

7.2.6 Liaising with the registered provider and to implement arrangements for safeguarding data subjects' personal data and to make changes as appropriate where there are any adverse events or concerns related to the safety, privacy and confidentiality of personal information.

7.2.7 Conducting risk assessments related to hazards and risks associated with information governance and including these risks as appropriate on the risk register.

7.2.8 Ensuring that all staff receive information on induction about records management and data protection arrangements in accordance with their roles and responsibilities.

7.2.9 Ensuring that all staff receive any required information and/or training about records management and data protection where there are any changes in practice in this area or where the results of quality and safety monitoring in St Peters identify the need for same.

7.2.10 Ensuring that allied healthcare professionals involved in the care of residents are aware of the arrangements in St Petersfor the safe and effective use of personal data.

7.3 **Responsibilities of Administration Staff**

7.3.1 The administration staff will have responsibility for the archiving and disposal of all manual records as per policy. The records will be logged on data base prior to being archived with external company.

7.3.2 All computer records will be managed by the Person in Charge/Data Controller/Data Protection Lead and external Consultant contracted to St Peters see point 14.2.

ARTICLE 29 DATA PROTECTION WORKING PARTY Guidelines on Data Protection Officers ('DPOs'), 2017 *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048*

7.4 **Responsibilities of Data Protection Lead**

The Data Protection Lead for St Petersis the Clinical Operations Manager. They are responsible for:

7.4.1 Informing and advising the registered provider and staff in St Peters of their obligations under data protection legislation.

7.4.2 Monitoring compliance of St Peters with legislation governing the use of personal data and special categories of personal data.

7.4.3 Providing advice and assistance as required in conducting data privacy impact assessments.

7.4.4 Cooperate with and act as a contact point for the Data Protection Commission on issues relating to processing.

7.4.5 Operate a risk based approach to monitoring compliance with legislation, prioritizing high risk processing activities.

7.4.6 Actively involved in the maintenance of the data register for Trinity Care.

7.4.7 Preparing all notices and privacy impact statements for Trinity Care.

7.4.8 For coordinating internal audits to ensure compliance with the GDPR.

7.4.9 For Coordinating the training of staff on their obligations on GDPR in conjunction with HR manager.

7.4.10 For ensuring all paperwork is collated and consented as per GDPR regulations.

7.4.11 For ensuring the external IT consultant has a contract in place and has signed appropriate confidentiality agreement.

7.4.12 For ensuring a contract exists between St Petersand all external sources that information is shared with.

7.4.13 For ensuring safe compliance with data disposal.

7.4.14 For ensuring all data breaches are reported as per GDPR.

7.4.15 To ensure all data is for limited purposes.

7.4.16 To ensure all staff are aware of their own integrity and confidentiality is maintained.

This list is not exhaustive.

7.5 **Responsibilities of Clinical Nurse Managers**

7.5.1 Supervision of nursing and care staff on a day to day basis to ensure that staff comply with the requirements of this policy.

7.5.2 Monitoring records management at floor level to ensure that practices comply with the requirements of this policy.

7.5.3 Carrying out audits of resident's records as directed by the person in charge.

7.5.4 Intervene where the security, privacy or confidentiality of any resident's personal data is at risk.

7.5.5 Feedback to the person in charge where there are any breaches of this policy or where there are concerns in relation to the arrangements for records management at floor level.

7.6 **Responsibilities of Staff Nurses**

Staff nurses have the following responsibilities:

7.6.1 Providing information to residents about the purpose of collecting personal information, who the information will be shared with prior to undertaking any assessments or collecting personal information from each resident.

7.6.2 Providing information about and documenting the resident's consent to the use and processing of personal information in accordance with this policy.

7.6.3 Ensuring that residents' healthcare records are accurate and complete with entries made in a timely fashion in accordance with the requirements of this policy.

7.6.4 Where a resident is unable to communicate consent, documenting same in the resident's healthcare record.

7.6.5 Where information is being collected from the resident's representative / next of kin, ensuring that an explanation of the purpose of collecting the information and proposed uses is given.

7.6.6 Reporting back to their line manager any concerns they may have regarding the safety and effectiveness of records management in Trinity Care.

7.6.7 Directing and supervising healthcare assistants in the completion of daily care records.

7.7 **Healthcare Assistants**

Healthcare assistants have the following responsibilities:

7.7.1 Complying with the requirements set out in this policy for records management in accordance with their role.

7.7.2 Complying with the requirements set out in this policy regarding the collection and use of personal data for residents.

7.7.3 Informing the nurse on duty or clinical nurse manager about any concerns they have regarding records management and the collection and use of personal information in Trinity Care.

7.7.4 Completing daily care records as outlined in this policy and as directed by registered nurses.

7.8 **All Staff**

7.8.1 All staff must comply with the requirements of this policy relevant to their roles.

7.8.2 All staff have a duty to safeguard the privacy and confidentiality of personal data obtained while the staff member is carrying out their role. Staff must not share this personal information except for the specific purpose for which the information is given.

7.8.3 Staff must only collect that personal information that is required by their role and responsibilities and in accordance with the requirements of this policy.

7.8.4 The personal identity or personal information about a resident/s must not be uploaded or discussed on any social networking site.

7.8.5 Staff are not permitted to photograph or video any resident, except for care and treatment documentation as outlined in this policy and in accordance with the requirements of this policy.

7.8.6 All staff, whose role involves the maintenance of records must ensure that these records are accurate, complete and up to date.

7.8.7 Maintain the confidentiality of all information related to the operation of Trinity Care.

8.0 Safeguarding Rights of Data Subjects in Trinity Care

8.1 **Information Rights**

Under data protection legislation, data subjects have the right to have the following information provided to them at the time that their personal data is obtained:

a) The name and contact details of the data controller.
b) The name and contact details of Data Protection Lead.
c) The purposes for which St Peters will use the personal data and the legal basis for same.
d) The length of time for which personal data will be stored;
e) Any other persons or organisation that will receive your data; for example, other healthcare staff; the Health Information and Quality Authority as part of an inspection process.
f) Whether personal data will be transferred outside the EU.
g) The data subject's rights, including the right to lodge a complaint with the Data Protection Commission and the right to withdraw consent at any time where the personal data has been obtained solely on the legal basis of consent.
h) The existence of automated decision-making and the logic involved, including the consequences thereof.

St Peters has the following measures in place to safeguard each data subject's right to information:

1. St Peters has prepared a privacy statement that provides an outline of how personal data is obtained and processed.
2. A copy of the privacy statement is given to each resident or member of staff on admission or commencement of employment with Trinity Care.
3. A copy of the statement is included in both the Statement of Purpose and Function and the Residents' Guide.
4. Written Consent is obtained when signing the contact of care on admission as our Data obligations forms part of the contract as well as giving and talking through the privacy notice with the resident/NOK. It must be noted that processing can take place not based on consent as per Article 9 of the Data Protection Act 2018.
5.

8.2 **Access Rights**

8.2.1 All data subjects have the right to obtain confirmation as to if personal data concerning him or her are being processed and where that is the case, the data subject has the right to obtain access to the personal data.

8.2.1 Under the Health Act, 2007 (care and welfare of residents in designated centres for older people) regulations 2013, a resident can access their care plan, provided it does not infringe on the rights of other data subjects.

8.2.2 A resident or any other individual who believes that their personal data is being processed by St Peters can make a request in writing for information about their personal data.

8.2.3 Requests for information about personal data being processed by St Peters should be made in writing to the Clinical Operations Manager, Data Protection Lead.

8.2.4 Upon receipt of a request for information about personal data being processed, the Data Protection Lead will confirm the identity of the person making the request and will provide the following information to the requestor:

1. A description of the purpose and legal basis for the processing of the data subject's personal data
2. A description of the categories of data being processed.
3. A description of those persons or organisations to whom the data subject's personal data has been disclosed.
4. The exact time period for which the personal data will be retained or where it is not possible to provide the exact time period, the criteria used by St Peters to determine the time period(s) for which personal data will be disclosed.
5. Information about the right of the data subject to request rectification, restriction or erasure of their personal data.
6. Information about the right of the data subject to lodge a complaint with the Data Protection Commission and contact details of the Commission.
7. Information about the origin of the personal data being processed, subject to the restrictions outlined in 8.3.

8.2.5 Where a data subject makes a request for information about personal data being held about them by Trinity Care. The Data Protection Lead will respond to the request and provide the information no later than one month after the date that the request has

been made, unless additional information is required from the requestor to either confirm their identity or to locate any relevant personal data.

8.2.6 Where the Data Protection Lead has reasonable doubt as to the identity of the person making the request, he/she may request additional information from the requestor to confirm their identity.

8.2.7 In exceptional cases, where the Data Protection Lead is of the opinion, that additional time will be required to consider a request, they may need to extend the time period, they must inform the requestor in writing within one month of the date of the request and may extend the time period to no more than two months.

8.2.8 When responding to a data subject's access to personal data, Data Protection Lead must ensure the rights and privacy of other data subjects are safeguarded.

8.3 **Restrictions to Access Rights**

Restrictions to access rights of data subjects may be implemented where necessary:

a) If the information is kept for preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing / collecting any taxes or duties; but only in cases where allowing the right of access would be likely to impede any such activities.

b) If the information concerns an estimate of damages or compensation in respect of a claim against St Peters, where granting the right of access would be likely to harm the interests of Trinity Care.

c) If the information is back-up data as it would be unreasonable to expect St Peters to retrieve back-up copies of its personal information in responding to an access request

d) If the information is kept only for statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.

e) If the information would be subject to legal professional privilege in court.

f) A data controller is not obliged to comply with an access request if that would result in disclosing data about another individual, unless that other individual has consented to the disclosure. However, the data controller is obliged to disclose so much of the information as can be supplied without identifying the other individual, e.g. by omitting names or other identifying particulars.

g) Where the personal data relating to the data subject consist of expressions of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential.

h) The Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989) provide that health data relating to an individual should not be made available to the individual, in response to an access request, if that would be likely to cause serious harm to the physical or mental health of the data subject. A person who is not a health professional should not disclose health data to an individual without first consulting the individual's own doctor, or some other suitably qualified health professional.

i) The Data Protection (Access Modification) (Social Work) Regulations, 1989 (S.I. No. 83 of 1989) provide that social work data relating to an individual should not be made available to the individual in response to an access request, if that would be likely to

cause serious harm to the physical or mental health or emotional condition of the data subject.

In any situation where access is denied, the Data Protection Lead must advise the data subject of the reason invoked for the restriction either at the time access is denied or as soon as is advisable thereafter. In addition, only the part of the data subject's information likely to cause harm can be withheld, the rest of the personal data should be released in the usual way. The data subject has a right to appeal the restriction to the Data Protection Commissioner.

8.4 **Right to Rectification of Data**

Data subjects have the right to have personal data rectified without undue delay, if they feel that the data are inaccurate. Additionally, data subjects have the right to have incomplete data completed, including by means of providing a supplementary statement. In situations where the data subject, such as a resident does not agree with the professional opinion of a healthcare professional such as a diagnosis of depression, a supplementary statement by the resident outlining their disagreement with the professional opinion should be inserted.

8.5 **Right to Erasure**

8.5.1 Data subjects have the right to have personal data erased, without undue delay and no later than one month following the request in the following instances:

a) Where the personal data are no longer necessary in relation to the purposes for which they were obtained and processed.
b) Where the legal basis for processing was the consent of the individual, the individual now withdraws that consent and there are no legal or other overriding legitimate interest for continuing to hold the data.
c) The data subject objects to the processing and there are no overriding legitimate grounds for the processing or where the data subject objects to their personal data being processed for direct marketing purposes.
d) The data was processed unlawfully.

8.5.2 Where a data subject requests the erasure of their personal data, St Peters must inform any third-party processors of the need to erase the data, unless it is subject to any of the exceptions outlined in 8.6, or unless the erasure proves impossible or involves disproportionate effort.

8.6 **Restrictions to Right of Erasure**

The right of erasure shall not apply if the processing is necessary:

a) To comply with a legal obligation,
b) For a task carried out in the exercise of official authority vested in the controller,
c) For public interest in public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,
d) For the establishment, exercise or defence of legal claims.

8.7 **Right to Restriction of Processing**

8.7.1 A data subject has the right to obtain restriction of processing personal data in the following instances:

a) Where the accuracy of the data is contested by the data subject, for a period enabling St Peters to verify accuracy of the data.

b) The processing is unlawful and the data subject opposes erasure of their personal data and requests restriction of their use instead.

c) St Peters no longer needs the personal data for the purposes of the processing, but the data subject requires the data for the establishment, exercise or defence of legal claims.

d) The data subject has objected to processing, pending the verification whether the legitimate grounds of St Peters override those of the data subject.

8.7.2 Where the data subject has requested restriction of processing personal data, St Peters and specifically, Data Protection Lead, will communicate any restriction of processing to recipients of the personal data, unless this proves impossible or involves disproportionate effort.

8.8 **Right to Data Portability**

8.8.1 Data subjects have the right to receive personal data concerning them which they have provided to Trinity Care, in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller without hindrance from Trinity Care. This right applies where the processing is based on consent, or for the performance of a contract and the processing has been carried out by automated means.

8.8.2 In exercising the right to data portability, the data subject has the right to have the personal data transmitted directly from one controller to another. ***However, if a data subject requests the transfer of their personal data to another controller, written consent from the data subject must be obtained prior to any transfer, for example where a resident wants their personal data to be transferred to another healthcare provider.***

8.8.3 The right to data portability will not apply where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority invested in Trinity Care.

8.8.4 The right to data portability must not adversely affect the rights and freedoms of others.

8.9 **Right to Object**

8.9.1 A data subject has the right to object, on grounds related to his/her situation, at any time to processing of personal data concerning him or her which is based on

a) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority invested in Trinity Care.

b) Processing is necessary for legitimate interests pursued by St Peters or by a third party, except where such interests are overridden by the interests or fundamental freedoms of the data subject which require protection of personal data.

c) Where the data subject objects to processing for direct marketing purposes, the personal data will no longer be processed for such purposes.

d) Processing that is necessary for scientific, historical research or statistical purposes, unless the processing is necessary for the performance of a public interest task.

8.9.2 A data subject has the right not to be subject to a decision based solely on automated processing that would produce legal effects concerning him/her or similarly affects him/her.

8.10 **Third Party Processors**

St Peters engages third party processors to process personal data and special categories of personal data as part of its electronic records system in use. A written agreement is in place with each of these processors, which includes:

a) Sufficient guarantees provided by the processor to ensure that the rights and freedoms of the data subjects are safeguarded and that the measures are in place to ensure the processing complies with legislation.
b) The subject matter, duration, nature and purpose of the processing.
c) The type of personal data to be processed and the categories of data subjects to whom the personal data relate.
d) The obligations and rights of Trinity Care.
e) The provision that the processor will act only under the instructions of the Data Protection Lead.
f) The provision that the processor may only procure the services of another processor in relation to the processing, only where authorised to do so in advance and in writing by the Data Protection Lead/Officer.
g) The provision that the processor undertakes to maintain the confidentiality of the personal data or is under appropriate statutory obligation to do so.
h) That the processor will assist St Peters in ensuring compliance with data protection legislation.
i) That the processor will erase or return to Trinity Care, all personal data upon completion of the data processing services carried out by the processor on behalf of St Peters and erase any copy of the data, unless the processor is required by law to retain the data.
j) Provision that the processor will make available to St Peters all information necessary to demonstrate compliance with this section.

8.11 **Employee Confidentiality Agreements**

8.12 All staff employed by or contracted by St Peters must sign confidentiality agreements as part of their contract.

8.13 Staff leaving St Peters must have their access revoked, both to local and online applications and services, including backup services.

9.0 Record of Data Processing Activities

9.1.1 St Peters is required under Article 30 of the GDPR to maintain a record of data processing activities in Trinity Care. This is referred to as the Data Register and is maintained by the Data Protection Lead/and the PIC's.

9.1.2 The Data Register for St Peters includes the following information as required by legislation:

a) the name and contact details of the data controller and where applicable, the joint controller and the practice lead for data protection;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed;
e) where applicable, transfers of personal data to a third country;
f) the envisaged time limits for erasure of the different categories of data;
g) a general description of the technical and organisational security measures.

10.0 Data Protection Impact Assessment (DPIA)

Under Article 78 of the GDPR, St Peters is obliged to conduct a data protection impact assessment where processing and any new type of processing using technology is likely to result in a high risk to the rights and freedoms of individuals.

10.1.1 Where there are any significant changes to how personal data is being processed, the *Data Protection Lead/coordinator/team* will carry out a threshold assessment of the change. The threshold assessment will determine whether the change involves:

1. The collection, use or disclosure of personal health information?
2. The collection, use or disclosure of additional personal health information held by an existing system or source of health information?
3. A new use for personal health information that is already held?
4. Sharing of personal health information within or between service providers?
5. The linking, matching or cross-referencing of personal health information that is already held?
6. The creation of a new or the adoption of an existing, identifier for individuals; for example, using a number or biometric?
7. Establishing or amending a register or database containing personal health information? New or innovative use of technology or organisational solutions?
8. Exchanging or transferring personal health information outside the European Union?

9. The use of personal health information for research or statistics, whether de-identified or not?
10. A new or changed system of data handling; for example, policies or practices around access, security, disclosure or retention of personal health information?
11. Any other measures that may affect privacy or that could raise privacy concerns with the public?

10.1.2 If the result of the threshold assessment is that a DPIA is not required, the process must be documented, signed off by the Registered Provider and stored in the project management file.

10.1.3 If the result of the threshold assessment is that a DPIA is required, the Data Protection Lead will carry out a DPIA.

10.1.4 The Data Protection Lead will decide on what personnel will need to take part in the assessment. This will be determined by the nature, scope, context and purpose of the change and may require the assistance of an external consultant with specific expertise. Methods for consulting with stakeholders will be decided at this stage.

10.1.5 This DPIA will commence with identifying potential privacy risks by examining how St Peters manages privacy and exploring the project's information flows with regard to individuals' fundamental right to privacy. Privacy management arrangements, a description of the project and mapping of information flows will be recorded on the DPIA form. The project team will use the guidance for DPIAs provided by the Health Information and Quality Authority, (2017) when completing the DPIA.

10.1.6 The DPIA process must commence at the planning stage of any new or significantly amended programme, initiative, system or project that involves the collection, use or disclosure of personal health information in Trinity Care.

10.1.7 Consultation with stakeholders form an important part of the DPIA and the Data Protection Lead will decide as to who are the stakeholders and what method of consultation will be used when a DPIA is carried out.

10.1.8 If there is a residual or remaining 'high risk' which cannot be mitigated, the Data Protection Lead must consult the Office of the Data Protection Commissioner for advice and the project team should decide if it is acceptable to continue with the project.

10.1.9 On completion of the DPIA, where it is decided to continue with the change project, the Data Protection Lead will:

a) Write up each stage of the DPIA in a report and include an action plan for implementation of the change, which addresses any issues raised by the DPIA.
b) Include any privacy risks in Trinity Care's risk register including the risk rating, measures in place to mitigate the risks and any additional measures to be implemented.
c) Continue to monitor the privacy risks as part of the risk management system in St Peters and specifically where safety or quality information identifies any issues with privacy or where there is any change to practice in this area.

11.0 Responding to a Data Breach

11.1 Personal Data Breach

11.1.1 A personal data breach is a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (GDPR)

11.1.2 "Destruction" of personal data is where the data no longer exists, or no longer exists in a form that is of any use to the controller (Article 29 Data Protection Working Party, 2018)

11.1.3 "Damage" is where personal data has been altered, corrupted, or is no longer complete (Article 29 Data Protection Working Party, 2018)

11.1.4 "Loss" of personal data, is interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession (Article 29 Data Protection Working Party, 2018)

11.1.5 Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR (Article 29 Data Protection Working Party, 2018)

11.1.6 Breaches can be categorised as:

1. "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
2. "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
3. "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of personal data.

11.1.7 Depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

11.1.8 A security incident resulting in personal data being made unavailable for ***a period of time*** is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. A breach involving the temporary loss of availability should be documented in accordance with Article 33(5).

11.1.9 Where personal data is unavailable due to planned system maintenance being carried out, ***this is not a 'breach of security' as defined in Article 4(12)***

11.1.10 Under Article 33 of the GDPR, when St Peters becomes aware of a personal data breach, it must be reported to the Data Protection Commission without undue delay and not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. Where St Peters does not notify the Data Protection Commission within 72 hours, the late notification must be accompanied by a written explanation of the delay.

11.2 Procedure for Responding to an actual or suspected breach of personal data

11.2.1 All staff employed by or contracted to Trinity Care, including processors must report any suspected or actual personal data breaches to the person in charge or his/her deputy immediately. Personal data breaches may include:

- A resident's record has been left in an area that is unsecured and accessible to persons who are not authorised to view the record e.g. in a resident's bedroom or in a main entrance foyer.

- A laptop containing personal data of residents or staff members has been left open in an area where it is accessible to persons, such as visitors who are not authorised to view the personal data.
- An unencrypted USB that contains personal data has been lost.
- There are indications that there has been a possible intrusion into Trinity Care's network
- A third-party informs a staff member that they have accidentally received the personal data of one of its residents or employees and provides evidence of the unauthorised disclosure.
- Information about an individual has been sent to the wrong department or organisation.

11.2.2 When the person in charge or his/her deputy is informed about a possible personal data breach, he/she must inform the registered provider and/or the data protection lead immediately.

11.2.3 The registered provider or the Data Protection Lead will immediately undertake an initial investigation to ascertain if a personal data breach has occurred. It is only when this has been completed that St Peters is considered as being aware of the breach

11.2.4 If the investigation determines that in fact a personal data breach has occurred, the Data Protection Lead must complete a first notification to the Data Protection Commissioner no later than 24 hours after detection of the breach. If all the necessary information is not available at the time of the first notification, a second notification must be made within 3 days of the first notification.

11.2.5 If the investigation determines that in fact a personal data breach has occurred, the registered provider and the Data Protection Lead will carry out an assessment to determine the risk to the rights and freedoms of the data subject(s) resulting from the breach as outlined in **11.3.**

11.2.6 Where it is determined that a data breach is unlikely to result in a risk to the rights and freedoms of data subjects, St Peters is not required to notify the Data Protection Commission. However, **a log of all data breaches must be maintained by** Data Protection Lead **as part of the data protection and risk management systems in Trinity Care. Under GDPR, "*The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."***

11.2.7 Where it is determined that the data breach has occurred, it is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Lead will identify and implement action(s) needed to address the breach.

Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has informed it of the breach (Article 29 Working Group, 2018).

11.3 **Assessment of Risk to the Rights and Freedoms of Data Subjects**

11.3.1 When assessing the risk to individuals as a result of a breach, the Data Protection Lead/Officer will consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. Article 29 Working Party, 2018 recommends that the assessment should take into account the following criteria:

- **The type of breach**: The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.
- **The nature, sensitivity, and volume of personal data**: when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. A combination of personal data is typically more sensitive than a single piece of personal data. Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.
- **Ease of identification of individuals:** An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Use of encryption or pseudonymization of personal data that has been breached can lower the risk of identifying individuals.
- **Severity of consequences for individuals**: Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm. Whether St Peters is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk.
- **The permanence of the consequences for individuals,** where the impact may be viewed as greater if the effects are long-term.
- **Special characteristics of the individual,** such as an individual who is particularly vulnerable.
- **Special characteristics of the data controller,** for example, a nursing home will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.
- **The number of affected individuals.**

11.3.2 When assessing the risk that is likely to result from a breach, the Data Protection Lead/Officer should consider a combination of the severity of the potential impact on

the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the Data Protection Lead/Officer should err on the side of caution and notify.

11.4 **Notifying Data Subjects of a Personal Data Breach**

11.4.1 Where a personal data breach is assessed as likely to result in a **high** risk to the rights and freedom of an individual, the Data Protection Lead will notify the data subject to whom the data breach relates, unless:

- appropriate technological and organization measures were in place would render the data intelligible to any person not authorised to access it.
- Measures have been taken by St Peters in response to the breach that ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialize.
- It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place.

11.4.2 Notifications made directly to data subjects without undue delay and must describe in clear and plain language:

- a description of the nature of the breach;
- the name and contact details of the data protection lead or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

11.4.3 Information must be given in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them.

12.0 Protocol for the Management of Residents' Personal and Healthcare Information

12.1 **Obtaining and using personal information for assessment and care planning**

12.1.1 As part of the pre-admission arrangements for residents in Trinity Care, personal information about a prospective resident may be obtained from them, a relative, legal representative or a third party such as another healthcare facility at the referral stage. The purpose of obtaining this information is to assist with making arrangements for a pre-admission assessment of the prospective resident's needs to be carried out in accordance with Health Act, 2007 (Care and Welfare of residents in designated centres for older people) regulations 2013.

12.1.2 A pre-admission assessment is carried out by the Person in Charge or their nominee for each prospective resident prior to admission. The nurse manager conducting the pre-admission assessment must inform the prospective resident of the purpose of this assessment, how the information will be used and with whom this information may be shared. The nurse manager will also ask the prospective resident about any preferences he/she has for sharing information with others, such as family members. The provision of this information, the resident consent to the use of the information and any preferences expressed by the resident must be recorded by the nurse manager in the relevant section of the pre-admission assessment form.

12.1.3 Where a prospective resident is unable to communicate their consent to the use of personal information, the nurse manager must record this on the pre-admission

assessment form. The nurse manager will then gather information from other sources as required to complete the assessment of needs. These sources may include other healthcare professionals involved in the prospective resident's care, the prospective resident's healthcare records and the views and observations of family members and/or representative.

12.1.4 On admission, each resident must be informed how their personal data will be used, including whom information will be shared with using the Privacy Notice. The resident's consent to the use and sharing of their personal data should be recorded on the Privacy Notice, signed and dated by the resident and a copy kept on their file

12.1.5 Where the resident is unable to communicate his/her consent to the processing of their personal information, this should be documented in the resident's record and their next of kin will be asked to sign on their behalf.

12.1.6 Each nurse who completes ongoing assessments must inform the resident of the purpose of the assessment and seek their permission to continue.

12.1.7 Where a resident has any preferences regarding the sharing of information, the nurse must also document these preferences in the resident's care plan.

12.1.8 Personal and healthcare information should be collected directly from the resident rather than from third parties as far as it is reasonable and practicable to do so.

12.1.9 All healthcare professionals who obtain personal information while conducting assessments and care plans for residents are obliged to inform the resident of the purpose of obtaining information and seeking the resident's permission to proceed with obtaining personal data. The resident's consent to assessments should be recorded in the resident's record maintained by the healthcare professional.

12.1.10 Only relevant information should be obtained from a resident, that is, the personal data must be required for a specific lawful purpose, such as for assessment and care planning to meet the resident's healthcare needs.

12.2 **Use and Processing of Residents' Personal Data**

12.2.1 A resident's personal data must only be used for the purposes for which the resident consented or where the resident has been unable to consent, the personal data may only be used for the purpose for which it was lawfully obtained.

12.2.2 Each healthcare professional obtaining and using personal data of residents has a duty of confidentiality to the resident and must only use the information for the purposes for which it is obtained.

12.2.3 Every healthcare professional, administrative or healthcare staff who obtains personal and/or healthcare information from or about residents must ensure that the information is obtained and processed fairly. Residents and/or their representatives must be informed of the purposes of obtaining the information including how the information may be used.

12.2.4 Information collected must be accurate, complete, up to date and organised.

12.2.5 Information will be held no longer than is necessary in accordance with the retention and disposal of records requirements outlined in this policy.

12.2.6 Residents' personal and healthcare information must be recorded in the designated records as outlined in this policy.

12.2.7 Records containing personal information must be stored in the designated areas outlined in this policy.

12.2.8 Where St Peters engages a third party to provide services on its behalf and where the services will require the service provider to process personal data, St Peters is required

by law to have a written contract in place with the service provider which provides sufficient guarantees regarding data protection compliance.

12.2.9 St Peters have contract in place for IT support and cloud storage of all personal data.

12.2.10 When a resident is no longer residing in St Peters or has passed away, the right of access by healthcare staff to the healthcare record is normally terminated. Access may still be authorised for purposes other than service user care, such as clinical audit, FOI/DP access, research or legal proceedings.

12.2.11 The Health Information & Quality Authority was established under the Health Act 2007. Its statutory functions are to set standards on safety and quality relating to designated centres for older people. It may also carry out inspections of certain services. Section 12 of the Health Act 2007 entitles HIQA to require a service provider to provide it with any information or statistics that HIQA needs to determine compliance with safety and quality standards.

12.2.12 Residents and/or staff information must not be discussed in areas either among staff or by telephone where it is likely to be overheard.

12.2.13 Personal information should not be given over the telephone unless it can be clearly established that the caller is whom they claim to be and proof of identity is essential. Staff must exercise caution and reasonable care in such cases, for example, checking with the caller for a payroll reference number, or a date of birth or mother's maiden name. It may also be appropriate to take a caller's telephone number, and then check the validity of the number by contacting the number back.

12.2.14 Personal information should not be left on voicemail/answering machine.

12.2.15 Mail containing personal information should be marked clearly with "Strictly Private and Confidential". If the information is particularly sensitive or proof of delivery is necessary, information of this nature should be sent by registered post.

12.3 **Records used in St Peters to store Residents' Personal Information**

St Peters stores and processes personal data in both electronic and manual format. The data register for St Peters outlines all categories of personal data that is obtained and processed for residents. Measures in place to safeguard residents' personal data is outlined under the relevant headings in the remainder of this policy.

12.4 **Information that must be stored in the Resident's Healthcare Records**

In accordance with statutory legislation and best practice, the following information is stored in resident's healthcare records:

- Name and contact details of the resident's next of kin; GP and other healthcare professionals involved in the resident's care in the residents' directory and each resident's healthcare record
- Initial screening, comprehensive and ongoing nursing assessments
- Nursing care plans
- Nursing progress and evaluation notes
- Risk Assessments
- Observations, daily care records, vital signs

- Referral letters, transfer letters and discharge communications and any other correspondence relevant to the care of the resident
- Medical and multidisciplinary clinical notes
- Consent forms
- Laboratory, radiology and diagnostic imaging results
- Prescribed medicines and nutritional supplements
- Appointments
- Care plan meetings with the resident and/or the resident's representative
- Multidisciplinary meetings
- Faxes sent or received relating to the care and treatment of the resident

This list is not exhaustive and the healthcare record must include any information related to the assessment, planning of care and treatment, delivery of care and treatment and monitoring of the resident's progress and response to care and treatment.

12.5 Information **Not** to be Included in Individual Healthcare Records:

The following information must not be included in a resident's healthcare record and must be stored in the appropriate record as outlined in **12.2.**

- Billing details - administration office
- Information related to complaints will be stored in the conference room in complaints book.
- Coroners Post-Mortem reports, unless consent from the coroner has been obtained, these will be stored in resident's file.

- Correspondence from solicitors which will be stored either in resident's file or in the administration office on Level 3.
- Data protection requests will be managed by Data Protection Lead and stored in the conference room.
- Financial information will be managed by administer and the accountant and all information is stored in the administration office.
- Garda reports will be stored in the administration office or resident's file.
- Health legal reports will be stored in resident's file.
- Incident report forms and risk management forms will be stored on care monitor and in the conference room in incident file.

NB: Information not included in the main healthcare record is subject to the same requirements for confidentiality and security as healthcare information.

13.0 Marking of Residents' Healthcare Records

13.1 Front Cover of Manual Records

13.1.1 Volume number, if more than one volume and the dates to which the records apply.

13.1.2 Resident identification details:

- First Name
- Middle Initial
- Surname
- Date of Birth
- Resident's Unique Identification Number

Alerts for all residents will be on the front cover of all manual records.

13.2 Additional Markings

Each resident has a unique identity number which is displayed on each page of their healthcare record.

13.3 Requirements for the Structure of Residents' Healthcare Records

13.3.1 Information must be recorded in chronological order and late entries identified as such. Scanned records must not include storage of more than one copy of each letter of correspondence unless notes have been made on both copies.

13.3.2 All healthcare professionals involved in the resident's care should determine the appropriateness of including sensitive information in the resident's records.

13.3.3 Where photographs are being used such as for resident identifier information, wounds, the resident's consent should be sought and documented as far as is practicable. The completed consent form should be stored in the resident's notes or scanned into care monitor.

13.3.4 The date of receipt must be recorded on all laboratory, radiological and diagnostic imaging reports and these must be signed as read and any action to be taken recorded by the resident's general practitioner/attending doctor.

13.4 **Storage of Residents' Healthcare Records**

13.4.1 All healthcare records are stored on EPIC care or in locked filing cabinets at the nurses station or in locked stores in each Home. Glenbeigh is Trinity Cares external achieving company and St Peters has contacts with them.

13.4.2 Electronic records are accessible in the following:

- Computer terminals based at each nurses' station.
- Computer terminals in the PIC's and ADON office. MDT and Clinical Operations Manager Laptops

13.4.3 IT company - Vital has a contract with St Peters to ensure compliance with GDPR and the safeguarding of our residents' data. St Peters do not have a cloud based storage but rather, all information is stored on a server based at Head office in Gormanston Wood Co. Meath

13.4.4 All staff with access to computerised system in St Peters have a responsibility to ensure that they use the computers only for the purpose for which they are provided. No staff member may use any computer for any personal or business use not associated with their work or for any illegal activity or usage.

13.4.5 All staff members with access to electronic communications in St Peters are expected to do so responsibly, that is, to comply with legislation and Trinity Care's policies and procedures governing records management and with normal standards of professional and personal courtesy and conduct.

13.4.6 Staff members must not install any software on any facility computer or use unauthorised software.

13.4.7 External users and/or suppliers of computer materials must comply with the requirements of this policy.

13.4.8 Staff members may not download any material from the internet that is obscene, vulgar or pornographic.

13.4.9 Disciplinary action may be taken, where a staff member is found to have used Trinity Care's computer system for any of the above-mentioned uses.

13.4.10 All healthcare records are stored in designated files in the nurses' office.

13.4.11 Access to healthcare records is limited to healthcare staff pertinent to their role and in keeping with the resident's preferences for sharing of information.

13.4.12 Healthcare records must not be left unattended on countertops or shelving. Following use, they should be returned to the designated secure storage area. Failure to return records to their designated secure area may result in a data breach.

13.5 **Privacy and Confidentiality of Residents' Information**

13.5.1 All computers in St Peters are access limited and password protected.

13.5.2 Password knowledge is limited only to those authorised to gain access to the data.

13.5.3 St Peters has a written license agreement with EPIC Care which provides details of confidentiality, storage and backup of records.

13.5.4 All staff members must ensure that their password is confidential and are not permitted to give their password to another member of staff.

13.5.5 Passwords must be of at least eight characters and changed every 90 days.

13.5.6 Access to special categories of personal data is controlled and allowed only in accordance with each staff member's requirement to access these categories of data in accordance with the staff member's role and responsibilities. A log is maintained and updated by the PIC quarterly.

13.5.7 All computers and laptops used to process personal data are encrypted.

13.5.8 All staff employed or contracted by St Peters(or representative officers of statutory bodies) who have access to records must uphold the right of privacy to persons who provide personal data/healthcare information even after a resident has been discharged or has passed away.

13.5.9 Personal data / healthcare information may only be used for the purposes for which it was provided, except in those specific circumstances outlined.

13.5.10 During everyday duties, nurses and other allied healthcare professionals must use professional judgment as to the appropriateness of sharing personal and/or sensitive data with others in accordance with the specific purpose for which the data has been provided, requirements for consent and the exemptions identified.

13.5.11 Information should only be given to the resident's next of kin / nominated representative with the consent of the resident. Where a resident has cognitive impairment, staff should comply with the requirements of the consent and advocacy policy.

13.5.12 **Healthcare information / advice must only be given to residents by a healthcare professional with the relevant authority.**

13.5.13 Staff must not leave any laptop or manual documentation containing personal information where it could be viewed by unauthorized persons.

13.5.14 All laptops and manual documentation must be stored in the designated areas.

13.6 **Access to Healthcare Records**

Healthcare records or their contents should only be made available to:

13.6.1 Those medical, nursing and healthcare staff that have responsibility for providing or supervising the resident's care.

13.6.2 Employees of St Peters or contracted staff who have authorisation to file, process, review the record for quality assurance, risk management or infection control purposes.

13.6.3 Healthcare professionals to whom the resident is being referred.

13.6.4 Authorisation to access healthcare records or contents may be given for research purposes where the resident's details are anonymised and in accordance with the requirements of informed consent.

13.6.5 Where nursing staff are unsure of any individual's right to access a healthcare record, he/she should liaise with the Person in Charge or his/her deputy and/or Trinity Care's legal advisors.

13.7 **Administrative Access to Healthcare Records**

13.7.1 Residents should have access to their nursing care plan if they request same. Care planning will be developed in consultation with the resident as far as he/she is able and therefore, the resident is entitled to access his/her care plan at all times.

13.7.2 Requests for access to healthcare records other than the nursing care plan must be made in writing to the Person in Charge or her designated deputy in her absence as well as the attending General Practitioner / clinician. Additionally, requests should:

- Specify the actual documents to which access is requested.
- Involve the relevant healthcare professional in handling the application to ensure that only information relevant to the application is released and the information is given in the correct manner and format and by the most appropriate healthcare professional.

13.7.3 Conditions under which access may be refused are outlined in **8.3**

(Where a request for information is refused under the above exceptions, requesters should be informed of their rights under the Data Protection Act.)

13.8 **Disclosure of Personal Health Information**

Personal health information should be used only for the purpose for which it was collected and may only be used or disclosed for any other purpose under the following conditions:

a) The resident has given consent to the proposed use or disclosure.

b) The healthcare professional has a reasonable belief that the use/disclosure is necessary to prevent a serious threat or danger to the life, health or safety of an individual or to public health and/or safety.

c) The use / disclosure has been authorised by law.

d) In the case of a resident who is incapable of giving consent where the information is disclosed to enable the provision of appropriate care or treatment and where this information is given to a person responsible for the resident.

e) Where disclosure of notifiable diseases is required.

f) Where disclosure is made to the Gardaí in relation to a criminal investigation.

g) For research or statistical purposes ***only*** where the data has been anonymised or aggregate data, from which individual residents cannot be identified. Residents should be informed in advance of such uses of their personal data. However, such uses of personal data are permitted, even where the resident was not informed in advance, provided that no damage or distress is likely to be caused to the individual (Data Protection Commissioner accessed 14/05/2018 https://www.dataprotection.ie/docs/The-Medical-and-Health-Sector/0/245.htm

h) If resident details are urgently needed to prevent injury or other damage to the health of a person, then the details may be disclosed. Section 8(d) of the Acts makes special provision for such disclosures. However, if the reason for the disclosure is not urgent, then consent must be obtained in advance (Data Protection Commissioner accessed

14/05/2018
https://www.dataprotection.ie/docs/The-Medical-and-Health-Sector/0/245.htm
(Data Protection Acts 1998 and 2003; Health Information and Quality Authority, 2012).

13.9 Disclosure of Information by Telephone / Fax

Where confidential personal information must be sent by fax, the following conditions must be observed:

- There are no other means of sending the information.
- It is an emergency situation.
- The fax must be sent from a fax machine that is located in locked cupboard in nurses' stations.
- Only registered nurses who are fully aware of their duty of confidentiality can send a fax containing personal health information
- A cover note is sent with the fax and only required information sent.
- When sending confidential information by fax, the security of the receiving fax should be established by phone call prior to the transfer of information and the person sending the fax should establish immediately after that the information has been sent to the intended recipient.
- ☞ Confidential information being disclosed by phone should only be disclosed by personnel who are authorised to do so, such as the Person-in-charge or senior nurse on duty and only given to personnel authorised to receive it.

13.10 Use of E-mail

Any document that contains personal health information about a resident must not be transmitted to other health providers by e-mail, unless an encryption pathway is available such as with Healthmail or Healthlink.

13.11 Employee Information and Staff Files

13.11.1 In accordance with statutory requirements, the Person in Charge of St Peters must maintain a record of all persons currently and previously employed at the centre.

13.11.2 Employees and potential employees have the same rights as any data subjects under data protection legislation. This includes right to information at the time of obtaining personal information.

13.11.3 Where personal data is obtained from a potential employee or an employee, the Data Controllor must ensure that the employee signs the privacy statement confirmation form outlining that he/she has been given information about the purpose of obtaining his/her data, how the data will be used, recipients of the data, retention periods and the rights of data subjects.

13.11.4 In the context of recruitment, personal data is obtained from potential employees to make a decision about their suitability for positions available. This information, including interview notes will be retained for a period of 12 months from the last data of contact, or longer where the information may need to be retained for pending legal cases.

13.11.5 In Trinity Care, each employee has a file created and maintained, which must include:

- The date on which the employee commenced and ceased employment.
- The position the employee holds in St Peters and the work that he or she performs, which is outlined in the contract of employment.
- A record of staff training which is recorded on the training matrix for St Peters and individual certificates placed in each employee's file.

13.11.6 The following information must be obtained and filed in each staff member's file in accordance with Trinity Care's Recruitment Policy:

- Evidence of the person's identity, including his or her full name, address, date of birth and a recent photograph.
- A vetting disclosure in accordance with the National Vetting Bureau (Children and Vulnerable Persons) Act 2012 and supporting documentation.
- Details and documentary evidence of any relevant qualifications or accredited training of the person.
- A record of current registration details of professional staff subject to registration.
- A full employment history, together with a satisfactory history of any gaps in employment.
- Correspondence, reports, records of disciplinary action as per policy and any other records in relation to his or her employment.
- Details of any previous experience (if any) of carrying on the business of a designated centre.
- Two written references, including a reference from a person's most recent employer (if any).

13.11.7 Each employee must have a signed contract of employment , which must be kept in the employee's file.

13.11.8 Any unsolicited applications received through all mediums will be destroyed if deemed unsuitable

13.12 Duty Rosters

13.12.1 The Person In Charge and or a person designated by them creates staff duty rosters, which includes details of the hours to be worked by employees in Trinity Care.

13.12.2 Changes to rosters, such as absence or sick leave must be made on the staff roster, Person-in-charge to ensure that there is a record of actual hours worked by employees in Trinity Care.

13.12.3 A copy of the duty rosters must be kept in nurses' station.

13.12.4 Information kept in staff files is confidential and can only be created, accessed or processed by the Person-in-charge, Administration, ADON, Clinical Operations Manager and the HR Director.

13.12.5 Other persons, who are authorised by law may also access staff files, such inspectors of the social services inspectorate who have legal authority under the Health Act (2007).

13.12.6 Personal information, including personal health information obtained from employees is subject to the provisions of data protection legislation.

13.13 General documentation

In accordance with schedule 4 of the care and welfare regulations (2013), St Peters also creates and maintains additional records.

13.13.1 A copy of the current statement of purpose and resident's guide has been prepared and a copy is displayed. The statement of purpose is reviewed on an annual basis or where there are changes to the purpose and/or function of the Home.

13.13.2 A copy of all inspection reports is kept in a designated folder and available for viewing by residents on request.

13.13.3 A record of the charges to residents, including any extra amounts payable for additional services not covered by those charges are outlined in the contract of care. The amounts paid by or in respect of each resident are kept in the administration office.

13.13.4 Records of the food provided for residents and of any special diets prepared for individual residents is kept in the kitchen and maintained.

13.13.5 Menus are displayed in the dining room and additional information regarding food intake for residents is recorded in food intake charts as required by the individual needs of each resident in their personal healthcare records.

13.13.6 A record of all complaints made by residents or representatives/relatives or by persons working at the designated centre about the operation of the designated centre are created in accordance with our Complaints policy. Records of complaints and the action taken by the person in charge in respect of any such complaint is kept in the PIC's office.

13.14 Notifications

In accordance with statutory requirements, the Person in Charge or deputy must complete and send notifications to the Chief Inspector. A record of all notifications completed and sent to the Chief Inspectors are filed in the PIC's office.

13.15 **Fire Safety Records**

13.15.1 The PIC maintains a fire policy and fire register for the Home, which outlines the arrangements for the prevention and detection of fire as well as the procedures to be followed in the event of fire.

13.15.2 A record of each fire practice, drill or test of fire equipment (including fire alarm equipment) conducted in the Home and of any action taken to remedy any defects found in the fire equipment is kept in the fire register.

13.15.3 A record of the number, type and maintenance record of fire-fighting equipment is also kept in the fire register.

13.16 **Directory of Visitors**

A record of all visitors is kept at the entrance to the Home. It includes the names of visitors, the date and time of entering and leaving the centre. A notice is displayed on the wall above the logbook reminding all visitors to sign in.

14.0 Retention and Disposal of Records

14.1.1 Records must be retained in accordance with the retention schedule outlined in Appendix 1.

14.1.2 Recommended retention periods should be calculated from the end of the calendar month following the last entry to the record.

14.1.3 Where any record due for disposal is known to be the subject of an access request, this contact will be regarded as the last contact date and the relevant retention period will apply.

14.1.4 Healthcare records should not be kept longer than the required retention period.

14.1.5 Disposal of records should safeguard the confidentiality of residents.

14.1.6 'Post it' notes and / or any scraps of paper that contain personal information related to a resident should be shredded prior to disposal.

14.2 **Disposal of Records**

14.2.1 All electronic information relating to the personal healthcare information of residents are stored on EPIC Care/Median Health Care which has an archiving system.

14.2.2 When the retention period for an electronic record containing personal data has expired, the Data Protection Lead/Controller will check to see if there is any additional

lawful purpose for which the data may need to be processed, as for example in legal cases.

14.2.3 Where there is no other legal basis for continuing to process the data, the Data Protection Lead/Controller will instruct by email EPIC Care/Median Healthcare to delete the record. They will in turn email back when the task is complete.

14.2.4 Staff and manual records are managed for storage and disposal by Glenbeigh.

14.3 The Data Protection Lead/Controller maintains a log of all records disposed of related to staff and residents of the home.

14.4 **Responsibilities of Glenbeigh who provide a Disposal Service**

14.4.1 The agency must use methods that both safeguard the confidentiality of healthcare records and comply with environmental health regulations.

14.4.2 The agency should sign a confidentiality agreement and provide a written certificate of proof of disposal.

14.4.3 A register of records destroyed must be kept. The register should contain the resident's name, date of birth, address, dates covered by the record, date of disposal and signature of the manager authorising disposal of the records. The signature of the second person who independently verified the need for disposal should be recorded on this register. The register of records should be stored in the administration office.

14.4.4 Disposal of healthcare records must comply with environmental health regulations.

14.4.5 The agency should have a license to dispose of records and this should be presented for confirmation to the nursing home.

To mitigate fire risk from paper particles, Glenbeigh outsources offsite shredding to Thornton's Recycling who are certified to BSEN15713 Secure Destruction of Confidential Material and ISO14001 Environmental Management. GRM formally audit Thornton's Recycling as part of our ISO9001 procedures. The Glenbeigh shredding process is outlined below:

- Boxes for destruction are picked from storage and their barcodes scanned, ensuring the correct boxes are selected.
- Boxes are brought to our internal shredding holding area and barcodes scanned to confirm all boxes to be shredded have been pulled.
- You can inspect the records before destruction.
- Boxes are transported to the secure shredding facility in Dublin 22 where you can witness the shredding.
- Shredding is carried out using a 'Double Shred' process, destroying documents beyond recognition.
- After shredding the relevant box status is updated to 'DESTROYED' on RS-SQL.
- A 'Certificate of Destruction' is provided to you.

Appendix 1

Type of Record	Retention Period	Disposal Arrangements.
Admission Record	7 years after the last entry.	As per local confidentiality arrangements.
General Healthcare including: Medical, Nursing, Allied health professionals.	7 years after the last entry.	As per local confidentiality arrangements.
Clinical Audit Records.	7 years.	Destroy under confidential arrangements.
Dental, ophthalmic and auditory screening records.	11 years	Destroy under local confidential arrangements.
Death, cause of, Certificates.	7 years.	Destroy under local confidential arrangements.
Serious untoward incidents including homicide.	30 years.	Destroy under local confidential arrangements.
Notifiable diseases records.	7 years.	Destroy as per local confidential arrangements.
Photographic material.	Should be retained as part of the resident's record for the period identified above.	
Documents/records related to any litigation.	Check with legal advisors.	Destroy under local confidentiality arrangements.
Records of Destruction of individual residents' healthcare records.	Permanent.	
Suicide.	10 years.	Destroy under local confidential arrangements.
Staff Records	7 years	Unless legislation states otherwise
Pre-assessment details of unsuitable resident	4 weeks	Destroy under Local confidential arrangements

Appendix 2

Potential Data Security Breach Report

Please complete the following questions in order to ascertain if a data security breach has occurred and return the completed form to the Data Protection Lead.

- **What type of data is involved?**

- **Does it fall within the definitions of Personal Data as outlined in 5.0 of the policy? If so, the following information must be provided:**

  - **Details of the breach**
  - **Date and time incident occurred (if known)**
  - **Date and time incident detected**
  - **Name of person reporting incident**
  - **Details on how the data was held e.g laptop, memory stick, computer hack**
  - **Details of safeguards if any, that would mitigate the risk if data has been lost or stolen.**
  - **Are there any reasons to suspect that the passwords used to protect the data may have been compromised? (E.g. password stored with mobile device or weak password used.)**
  - **Details of the number of individuals who's in formation is at risk i.e how many individuals personal data are affected by the breach?**
  - **Who are the individuals whose data has been breached – are they staff, residents, suppliers, third parties (families) etc?**
  - **What could the data tell a third party about the individuals?**
  - **Any other information**

Signed_____ **Date**_____

Appendix 3

TRINITY CARE

Resident Privacy Notice

St Peters make protection of your Personal Data a high priority, taking all appropriate measures to ensure your rights and data are protected. The statement below sets out what information we may keep on you, why we need it and how it is used, stored and destroyed when no longer required. We also set out contact details should you want further information or have any concerns.

Purpose of Holding Information

Information (data) about you is required, to enable us to understand and assess your individual needs and preferences and to assist us to provide the full range of nursing and care services you require.

The information we collect and process is required to:

- Manage our contract for care with you
- Comply with our Legal Obligations e.g. under the Fair Deal (NHSS Act 2009) or HIQA (Health Act 2007)
- Look after your Vital Interests in the event of an emergency
- Carry out our Legitimate interests in managing and running the nursing home

Information Held

In order for us to administer your contract for care and to comply with our statutory responsibilities under the law the type of information we hold about you while not exhaustive includes,

- A photograph
- A record of any accidents or incidents
- A record of any complaints raised by or about you
- Any correspondence to or about you
- Assessments (These may include the initial Comprehensive Assessment Form; a copy of the 'Fair Deal' Care Needs Assessment; Dependency Assessments; Individual Assessments on specific needs, e.g. continence, falls, nutritional assessments, etc)
- Care Plans
- Contract for Care
- Daily progress notes which outline information about your day-to-day care

- Decisions by you not to receive or refuse treatments
- Emergency contact information (including Next of Kin or other persons nominated by you)
- Entry in the Directory of Residents which includes specific information about you, your Next of Kin (or other appointed person), your GP, details about your admission or any temporary absence
- Financial information in relation to your 'Fair Deal' contribution and any additional fees payable under the contract of care or where we have been appointed as a 'pension agent' for you which may include your bank details; individual statements; invoices for care services provided; etc
- Medical Records (on admission and ongoing)
- Notification forms that we are required to send to HIQA
- Prescriptions and Medication Administration Records (including any medication errors or reactions you may have had to individual medicines)
- Records about your future wishes (e.g. advanced care plans; Do Not Attempt Resuscitation Orders; End of Life wishes)
- Records of any furniture or valuables you may have brought into the nursing home or deposited for safe-keeping
- Records of any visitors to the nursing home for you
- Referral Forms (to and from Allied Health Professionals e.g. hospitals, physiotherapists, dietitians, etc)
- Risk assessments (e.g. risks relating to your evacuation from the centre if there is a fire; smoking risk assessments; your risk of falls; etc.)

In addition, we may record images of you on CCTV for security and Health and Safety reasons. The use of CCTV falls within the scope of the Data Protection Act 2018.

In order to comply with the requirements of the Act, data must be:

1. Obtained and processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Information is collected only for one or more specified, explicit and lawful purposes
3. Information is kept safe and secure
4. Information is kept accurate, complete and up-to-date
5. Information is adequate, relevant and not excessive
6. Information is retained for no longer than is necessary for the purpose or purposes and according to legal requirements.

7. The Controller shall be responsible for, and be able to demonstrate compliance with, the 6 points above. (Accountability)

Due to some incidents of injury to staff members and for the safety and security of our residents and staff a recording system is used for ensuring the safety of residents and staff. CCTV is only in operation in communal areas of the Home

Access to Information

In order for us to provide you with the care you need, it may be necessary for us to liaise with a range of different health professionals and care services and therefore we will need to disclose specific information about you to third parties as highlighted above or where we are legally obliged to by HIQA. We will take all reasonable measures to ensure that your privacy and dignity is protected at all times during this process and will highlight to you if there are any exceptional instances where your information may have been compromised.

Access to information contained in your personal health record or other files relating to you, will only be by appropriate people in the nursing home. Some government bodies have a legal basis to inspect information contained in your records and the nursing home must make this information available to them. The nursing home may provide some of the information contained in your personnel file to third party (such as an IT company providing online care record systems). Some of this information may be stored on a cloud storage system and when this takes place your information will be protected with a Data Processing Agreement with the company and the cloud storage provider that complies with EU transborder data transfer rules.

Updating your Information

If at any stage the information you have provided changes (e.g. NOK contact details) we should be notified in writing, so our records can be updated.

Retention of Information

All information about you is required by law to be held during the time you reside with us and for a period of seven years after you leave the nursing home, after which it will be destroyed by Glenbeigh Records Management Damastown Way Damastown Business Park Dublin 15 and EPIC Care Services. Please refer to our retention and destruction records Policy for full details on how long we store your personal data and why

The Data Protection Contact

The Data Protection contacts for our nursing home is the Administrator/The Director of Nursing/Clinical Operations Manager

Your Rights in Relation to your Personal Data

You have certain rights in relation to your personal data. You have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

If you would like to see the information held on you by our Nursing Home or receive a copy of your personal data please make a Subject Access Request.

Should you have a concern about your information or how we manage it please contact the Data Protection Contact above. Should you not be satisfied with our response to your concerns or believe that we have not complied with our data protection obligations you may lodge a complaint with the Office of the Data Protection Commissioner

By signing below, you are happy for use to process your data.

Signature _____ Date_____

Appendix 4

Staff Privacy Notice

Dear Staff Member,

Following on from an insertion in our Employee Handbook 2017 regarding Data protection, this is a document to provide you with up-to-date information regarding the General Data Provision Regulations.

Privacy Notice

How your information will be used

1. As your employer, the Company (Trinity Care) needs to keep and process information about you for normal employment purposes. In the main the information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Company and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

2. As a company providing Residential Care activities, we may sometimes need to process your data to pursue our legitimate business interests, for example to prevent fraud, administrative purposes, safeguarding issues or reporting potential crimes.

The nature of our legitimate interests are in line with requirements and the Safeguarding of our Residents. We will never process your data where these interests are overridden by your own interests.

3. Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your supervisor, line-manager, colleague, resident, family member etc. or external sources, such as referees. We must have a reference from your most recent employer on file and another employer or professional person if you are providing a character reference .

4. The type of information we hold includes your application form and references, your contract of employment and any amendments to it; correspondence with or about you, for example, Garda Vetting, letters to you about a pay rise or, at your request; information needed for payroll, benefits and expenses purposes; contact and emergency contact details; night workers questionnaire; records of holiday, sickness and other absence; relevant medical information; and records relating to your career history, such as, education, qualifications, training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records, more information can be found in the Employee Handbook.

5. You will, of course, inevitably be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company.

6. Where necessary, we must be keep information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations - to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate.

8. In addition, we monitor computer use, we also keep records of your hours of work by way of our biometric system this information is for St Petersuse only and is not accessed by a third party. The information stored on Epic Care, E-MAR is in the main use for Residents records, however it will be accessed when required for internal and external auditing purposes and reviews.

9. Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to pension or health insurance schemes . If there is a Safeguarding issue raised we will in so far as is reasonably practicable meaning protect the identity of any staff member named.

10. We may transfer information about you to other St PetersHomes for purposes connected with your employment regarding a transfer temporarily or permanent or for educational purposes.

12. Your personal data will be stored in the Nursing Home while you are in employee. Should you become an ex-employee your data will be archived on-site after a period of time it will be sent to a secure global archiving company unless there are legitimate reasons otherwise . Your information it will be sent for archiving to a secure location for a period of seven years or the criteria used for determining how long your data will be stored for is as set out in legislation

14. If in the future we intend to process your personal data for a purpose other than that which it was collected we will provide you with information on that purpose and any other relevant information. This may be for research purposes or marketing, you will be kept informed and your permission sought in advance.

Your rights

15. Under the General Data Protection Regulation (GDPR) you have a number of rights with regard to your personal data. You have the right to request from us access to your personal data, you also have the right to rectify inaccurate personal data and restrict the processing of personal data.

16. If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn.

17. You have the right to lodge a complaint to the Information Commissioners' Office if you believe that we have not complied with the requirements of the GDPR or DPA 18 with regard to your personal data.

Identity and contact details of controller and data protection officer

18. The administrator in your Nursing Home is the controller of data for the purposes of GDPR.

19. If you have any concerns as to how your data is processed you can contact: The Administrator/Director of Nursing or Clinical Operations Manager

Yours sincerely

Susan McLaverty HR.