1.0 It is the policy of the Children's Sunshine Home, operating as LauraLynn, Ireland's Children's Hospice (the Service), as Data Controller, to endorse best practice in adhering to the legislative requirements of data protection as detailed in the Data Protection Acts 1988, 2003 & EU General Data Protection Regulation (GDPR) 2016.

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed in line with data protection principles and on a lawful basis.

GDPR promotes a risk-based approach to assessing risk when processing personal data. Many of the main concepts and principles of GDPR are much the same as those in the Data Protection Acts 1988 & 2003, however GDPR introduces new elements and significant enhancements which will require detailed consideration by the service in regard to processing personal data.

The purpose of this policy is to ensure the service safeguards the fundamental 'right to privacy' of the service and individuals, their right to exercise control over: what personal data is held; why and how it is used; and that the highest security measures are in place to ensure confidentiality.

2.0 Scope

2.1 All staff members in the organisation who collect or control the content and use of personal data of the service and individuals who avail of our services are responsible for compliance with the Data Protection Acts 1988, 2003 & EU General Data Protection Regulation 2016.

2.2 Partners and any third parties working with or for LauraLynn Ireland's Children's Hospice, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by LauraLynn Ireland's Children's Hospice without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which LauraLynn Ireland's Children's Hospice is committed, and which gives LauraLynn Ireland's Children's hospice the right to audit compliance with the agreement.

3.0 Definitions and Abbreviations

3.1 *Automated Data:* Broadly speaking, any information on a computer or information recorded with the intention of putting it on a computer.

3.2 *Child:* The GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 1/3 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

3.3 *Data:* Information in a form which can be processed. It includes both automated and manual data

3.4 *Data Controller:* Are those who, either alone or with others, controls the contents and use of personal data. Under the Data Protection Act, the Service is the Data Controller.

3.5 *Data Processor:* Is a person who processes personal data on behalf of a Data Controller, but does not include an employee of a Data Controller who processes such data in the course of his/her employment

3.6 *Data Subject:* A data subject is the individual the personal data relates to.

3.7 *Data subject consent*: 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.

3.8 *GDPR:* General Data Protection Regulation (2016/670) is the new EU Regulation on Data Protection, which came into force on 25th May 2018.

3.9 *Manual Data:* Information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

3.10 *Personal Data:* Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or likely to come into, the possession of the data controller. Personal data includes a person's photograph, CCTV/video recordings of person's image and recording of a person's voice (example list is not exhaustive).

3.11 *Processing:* Performing any operation or set of operations on data, including:

- Obtaining, recording or keeping data
- Collecting, organising, storing altering or adapting data
- Retrieving, consulting or using the data
- Disclosing the information or data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blocking, erasing or destroying the data

3.12 *Profiling:* is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

3.13 *Personal data breach*: a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject

3.14 *Relevant Filing System:* Any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.

3.15 *Special categories of personal data*: 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 the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.16 *Third party:* 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.

4.0 Responsibilities

4.1 *Chief Executive Officer (CEO):* Overall responsibility for ensuring compliance with the Data Protection Acts and where appropriate informing the Data Commissioner of any Data Protection breaches

4.2 *The Management Team and Departmental Managers:* Are responsible for compliance with the Data Protection Acts in their areas of responsibility and to ensure that all personal data held on computer or manually, is accessed only on a 'need to know' basis.

4.3 *Data Protection Officer:* Responsible for ensuring support, assistance, advice and training to all departments is available in order to ensure that they are in a position to comply with the legislation.

The data protection officer shall also be responsible for reviewing the register of processing annually in the light of any changes to Organisation Name's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request

They are also responsible for co-ordinating access requests and investigations under the Data Protection Acts.

4.4 *ICT Administrator:* Has responsibility for ensuring that all computer systems are compliant with the Data Protection Acts and for ensuring that the disposal of old computers is in accordance with the Data Protection Acts.

4.5 *All staff and volunteers:* Any individual who separately collects and/or controls the content and use of personal data are individually responsible for compliance with the legislation and the 'The Eight Rules of Data Protection'.

Any staff member who is assigned a laptop are responsible for keeping them secure particularly when in a public area. Laptops or other portable devices are encrypted and password protected. .

All staff members who hold personal data on Removable Media are responsible for keeping information secure particularly when in transit.

All staff members must report immediately, any breach of Data Protection legislation observed, to their line manager.

All staff members must be aware of the ten 'Rights of Data Protection'

All staff members must be aware of the procedure as per 6.0 below, especially on how to access Personal Data'.

All staff members must be aware of 'How a Complaint is made to the Data Protection Commissioner', as per 6.6.

Where a member of staff does not adhere to this policy and/or breaches the Data Protection Act, the individual may be subject to the Disciplinary Procedure.

5.0 Key Principles of Data Protection

5.1 The Service undertakes to perform its responsibilities under the legislation in accordance with the protection principles as outlined in Article 5 of the GDPR, which are as follows:

5.2 **Personal data must be processed lawfully, fairly and transparently**

Lawful: identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly: in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently: the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

5.2.1 The identity and the contact details of the controller and, if any, of the controller's representative;

5.2.2 The contact details of the Data Protection Officer;

5.2.3 The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

5.2.4 The period for which the personal data will be stored;

5.2.5 The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

5.2.6 The categories of personal data concerned;

5.2.7 The recipients or categories of recipients of the personal data, where applicable;

5.2.8 Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

5.2.9 Any further information necessary to guarantee fair processing.

5.3 **Personal data can only be collected for specific, explicit and legitimate purposes**
Data obtained for specified purposes must not be used for other purposes, save where the GDPR provides for same.

5.3.1 Personal data must be adequate, relevant and limited to what is necessary for processing

5.3.2 The Data Protection Officer is responsible for ensuring that service does not collect information that is not strictly necessary for the purpose for which it is obtained.

5.3.3 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

5.3.4 The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive

5.4 **Personal data must be accurate and kept up to date with every effort to erase or rectify without delay**

5.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

5.4.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

5.4.3 It is also the responsibility of the data subject to ensure that data held by service is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

5.4.4 Staff and families should be required to notify the service of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained in the services Records Management Policy. It is the responsibility of the service to ensure that any notification regarding change of circumstances is recorded and acted upon.

5.4.5 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

5.4.6 On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by the service, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with HSE's Retention of Records Procedure

5.4.7 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If the service decides not to comply with the request, the Data Protection must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

5.4.8 The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

5.5 **Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.**

5.5.1 Where personal data is retained beyond the processing date, it will be minimised in order to protect the identity of the data subject in the event of a data breach as per the HSE Retention of Records Policy

5.5.2 Personal data will be retained in line with the HSEs Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

5.5.3 The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in HSE Retention of Records Procedure, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

5.6 **Personal data must be processed in a manner that ensures the appropriate security**
The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of the service controlling or processing operations.

5.6.1 In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on the service itself, and any likely reputational damage including the possible loss of customer trust.

5.6.2 When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Identifying appropriate international security standards relevant to the service.

5.6.3 When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout the service
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

5.6.4 These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

5.7 **The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)**

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

5.7.1 The service will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

6.0 Data Subjects' Rights

6.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

6.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed (as per section 7.0).

6.1.2 To prevent processing likely to cause damage or distress.

6.1.3 To prevent processing for purposes of direct marketing.

6.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

6.1.5 To not have significant decisions that will affect them taken solely by automated process.

6.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

6.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

6.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

6.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

6.1.10 To object to any automated profiling that is occurring without consent.

6.2 The service ensures that data subjects may exercise these rights:

6.2.1 Data subjects may make data access requests as described in (section 7.0); this procedure also describes how the service will ensure that its response to the data access request complies with the requirements of the GDPR.

6.2.2 Data subjects have the right to complain to Organisation Name related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with [the Complaints Procedure].

7.0 Data Access Requests

7.1 Informal Access Requests

7.1.1 The Service's policy is to release personal data where appropriate without the need for the formal route of Data Protection. This ensures that access will be dealt with speedier than formal requests.

7.1.2 For access to records of a child/adult, who attends the Service, requests **must be in writing** (which can include email); addressed to the Director of Nursing or Head of Care. On occasion it may be necessary to ask for identification and proof of address.

7.1.3 The Director of Nursing/Head of Care shall inform the Data Protection Officer of the request to ensure the request is logged onto the Data Access Request Register

7.1.4 For access to records of the children/adults who are discharged, requests **must be in writing** (which can include email) and addressed to the Data Protection Officer. On occasion it may be necessary to ask for identification and proof of address.

7.1.5 Staff members who wish to request information in relation to their human resources/wages records should contact the Human Resources/Finance departments directly. Ex-staff **must put in writing** (which can include email) to the Human Resources Manager. On occasion it may be necessary to ask for identification and proof of address.

7.2 Formal Access Requests

7.2.1 If a person still wishes or prefers to make a formal access request the request must be addressed to the Data Protection Officer, (Please see Access Request Form Appendix 1).

7.2.2 Details that might be needed to help to identify the requester and to locate all the information that the Service may keep about you, should be included for example, date of birth, any previous addresses, what service you attended or where you worked including name(s) you were known by when in the Service. If you only want a small portion of the data please be specific as this will result in a speedier response.

7.2.3 The Service may on occasion require identification and proof of address before personal data will be released.

7.2.4 In response to an access request the Service must:

- Supply the information to the individual promptly and within 1 month of receiving the request;
- Provide the information in a form which will be clear to the ordinary person, e.g. any codes must be explained.

7.3 Where the Service does not keep any information about the individual making the request you should tell them so within 1 month.

7.4 If the Service restricts the individual's right of access in accordance with one of the very limited restrictions set down in the Acts, the Service must notify the data subject in writing within 1 month and must include a statement of the reasons for refusal. The Service must also inform the individual of his/her entitlement to complain to the Data Protection Commissioner about the refusal.

7.5 There are a number of modifications to the basic Right to Access granted by the Acts which include the following:

- Access to Health and Social Work Data: There are modifications to the right of access in the interest of the data subject or the public interest, designed to protect the individual from hearing anything about himself or herself which might cause serious harm to his or her physical or mental health or emotional well-being;
- In the case of Examinations Data: There is an increased time limit for responding to an access request from 40 days to 60 days and an access request is deemed to be made at the date of the first publication of the results or at the date of the request, whichever is the later.

8.0 Consent

8.1 The service understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

8.2 The service understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

8.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

8.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

8.5 In most instances, consent to process personal and sensitive data is obtained routinely by the service using standard consent documents e.g. when a family signs a contract, or a child's photograph is being taken.

9.0 Security of Data

9.1 All Employees/Staff are responsible for ensuring that any personal data that the service holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the service to receive that information and has entered into a confidentiality agreement.

9.2 All personal data should be accessible only to those who need to use it, and access may only be granted from their line manager or a senior member of staff. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with the services requirements and/or

9.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of the service. All Employees/Staff are required to maintain confidentiality before they are given access to organisational information of any sort, which details rules on screen time-outs.

9.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation by their line manager. As soon as manual records are no longer required for day-to-day support, they must be removed from secure archiving.

9.5 Personal data may only be deleted or disposed of in line with the HSE Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by Support I.T.

9.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

9.7 It is important to ensure that the children's/adult's family and/or staff information is not discussed in inappropriate areas where it is likely to be overheard including conversations and telephone calls. Particular care should be taken in areas where the public have access.

10.0 Disclosure of Data

10.1 The service must ensure that personal data is not disclosed to unauthorised third parties which could include family members, friends, government bodies, and in certain circumstances, relevant law enforcement bodies. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the services business.

10.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

11.0 Retention and Disposal of Data

11.1 The service shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected

11.2 The service may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

11.3 The retention period for each category of personal data will be set out in the HSE Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations the service has to retain the data.

11.4 The HSE Retention of Records Procedure will apply in all cases.

11.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the service's contract which is in place with SHRED IT.

11.6 All records that is disposed of shall be documented on the service's disposal register.

12.0 Data Transfers

12.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

12.1.1 An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

12.1.2 Privacy Shield

If the service wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

Assessment of adequacy by the data controller

In making an assessment of adequacy, the exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

12.1.3 Binding corporate rules

The service may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that the service is seeking to rely upon.

12.1.4 Model contract clauses

The service may adopt approved model contract clauses for the transfer of data outside of the EEA. If the service adopts the model contract clauses approved by the relevant supervisory authority there is an automatic recognition of adequacy.

12.1.5 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

13.0 Information Asset Register/Data Inventory

13.1 The service has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. The service's data inventory and data flow determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- all retention and disposal requirements.

13.2 The service is aware of any risks associated with the processing of particular types of personal data.

13.2.1 The service assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs), where necessary and are carried out in relation to the processing of personal data by the service, and in relation to processing undertaken by other organisations on behalf of the service.

13.2.2 The service shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

13.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, The service shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

13.2.4 Where, as a result of a DPIA it is clear that the service is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not the service may proceed must be escalated for review to the Data Protection Officer.

13.2.5 The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

14.0 Complaint to the Data Protection Commissioner

14.1 The Data Protection Commissioner will help to ensure that an individual's rights are fully upheld and the service meet their obligations under the Data Protection Act. If an individual feels that an organisation or individual is not meeting their data protection obligations and are not satisfied with their responses to concerns raised, a complaint can then be made to the Commissioner.

14.2 To make a complaint an individual should write or email the Data Protection Commissioner (address and email below) giving details about the matter and :

- Identify the organisation or individual complaining about;
- Outline the steps you have taken to have your concerns dealt with;
- Indicate the response received, if any, and
- Provide copies of any correspondence between the complainant and the organisation.

The office of the Data Protection Commissioner
Canal House
Station Road
Portarlington
Co Laois
LoCall: 1890 252 231
Tel: 057 868 4800
Email: info@dataprotection.ie
Website: www.dataprotection.ie

15.0 Personal Data Security Breach Code of Practice

15.1 Where an incident gives the service rise to a risk of unauthorised disclosure, loss, destruction, or alteration of personal data, in manual or electronic form, the Service must give immediate consideration to informing those affected.

Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. The data subject shall be contacted by the data controller using the Notice to Data Subject template (appendix 2) In appropriate cases, the service should also notify any other organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

15.2 If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it (encryption), the service may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures were of a high standard.

15.3 All incidents of loss of control of personal data in manual or electronic form by a member of staff must be reported to the relevant data controller as soon as the member of staff becomes aware of the incident. The Data Breach – Notice to Supervisory Authority template shall be used to notify the Data Protection Commissioner (see appendix 3).

15.4 All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the service becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected individuals **and** it affects no more than 100 people **and** it does not include sensitive personal data or personal data of a financial nature.

In case of doubt in particular any doubt related to the adequacy of technological risk-mitigation measures, the service should report the incident to the Office of the Data Protection Commissioner.

15.5 The service should make initial contact with the Office within 2 working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact may be by e-mail (preferably), telephone or fax and must not involve the communication of personal data.

The Office of the Data Protection Commissioner will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

15.6 Should the Office of the Data Protection Commissioner request the service to provide a detailed written report of the incident, the Office will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident;
- a chronology of the events leading up to the loss of control of the personal data; and
- the measures being taken to prevent repetition of the incident.

15.7 Even where there is no notification of the Office of the Data Protection Commissioner, the service should keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the service did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records should be provided to the Office of the Data Protection Commissioner upon request.

15.8 Where a member of staff does not adhere to this policy and/or breaches the Data Protection Act, the individual may be subject to the Disciplinary Procedure.

16.0 CCTV

16.1 The Service has signs posted in all areas covered by CCTV coverage to alert to the presence of cameras. CCTV tapes are handed over to An Garda Síochana, Ireland's National Police Service, in the event of a criminal offence.

The CEO, Facilities Manager and Quality, Safety and Risk Manager are the only persons authorised to review the CCTV within the Service. For further information please refer to the services CCTV Usage Policy (Ref No: 2.6).

17.0 Laptops

17.1 Only laptops issued by the Facilities Department can be used on the premises. No personal laptops are permitted for use on the site of LauraLynn with the exception of those designated areas where free guest Wi-Fi is available. Laptops allocated to specific staff members can only be used for service business.

17.2 Laptops must be shut down and/or locked away when not in use.

18.0 Computer Systems

18.1 Multi-level access control is present on all application software.

18.2 Access to computers must be restricted to authorised staff only and the information must be restricted on a 'need to know' basis. Confidential personal data on computer monitors must be kept unseen from any persons who are in the proximity of the computer and who should not have access to the information visible on the monitor

18.3 Systems must be password protected and screensaver password locked after period of inactivity (recommended duration of less than five minutes). Press 'Control, Alt and Delete' then click on 'Lock Computer'.

18.4 Individual computer user passwords must be kept confidential and changed regularly (recommendation to change passwords monthly). Passwords must never be disclosed to any person other than a staff member of the Support I.T Team for system maintenance. Before any outside engineer is given access to computers their identity must be confirmed.

18.5 In areas where computers are shared the password must only be given on a 'need to know' basis and changed regularly. Confidential documents containing personal data regarding children/adults,

staff members or public must be stored in a confidential password protected folder and accessed only by relevant staff.

18.6 It is expressly prohibited that users share application passwords (such as payroll software, HR software, accounting software etc.). In the event where a password is disclosed (deliberate or accidental), the user should immediately contact Support I.T to have the password changed or account disabled.

18.7 When a staff member leaves employment, information relevant to the service's business must not be deleted. This must be left on the centralised server storage (e.g. USERINFO Folder) where it can be accessed by the relevant Manager. It is the responsibility of all Managers to ensure that any departing staff members are aware of this procedure.

18.8 The service's systems are automatically backed up on network storage. Other important information should be backed up regularly. Contact the ICT Department for further advice.

18.9 Anti-virus software is in use and a dedicated hardware firewall is in place.

19.0 Emails

19.1 Emails containing personal data regarding a child/adult, staff member or a member of the public should not leave the internal email network. If an email is required to be sent or received from an external healthcare professional the authorised health mail accounts for the hospice and disability services shall be used.

Only authorised personnel shall have access to their emails outside of the service e.g. through mobile phones, remote access. Explicit consent shall be sought from the CEO or Head of Operations.

20.2 Emails are automatically saved on the Service's network server and when deleted are stored on the server indefinitely.

20.3 It is essential that all staff members with access to the email system retain important emails in its original state for record keeping purposes.

20.4 On individually assigned computers, if an email contains personal data regarding children/adults, staff members or public it should be safeguarded for future access. If relevant, the documents should be password protected. In areas where computers are shared, personal data should be printed off and filed in the main file or care plan. Information must then be deleted from the computer.

20.5 Any email which includes personal data should only be sent to one recipient unless deemed appropriate to inform multiple users.

20.6 Please ensure emails are sent to the correct person(s) particularly when choosing name(s) from a contact list. Where a breach occurs, the person shall be contacted immediately explained that the

intended use is not for them and ask for them to delete the email immediately. The Data protection Officer shall be informed off the breach immediately.

20.7 Emails re groups of people should not contain any personal data on any single child/adult/staff member/public – this should be sent separately in a separate email.

20.8 Emails should be saved and identified in such a manner to facilitate easy retrieval.

21.0 Printers/Photocopiers

21.1 If sending personal data to a centralised printer/photocopier a staff member must be present to collect printed documents with their own allocated swipe card. Sharing this card or asking another staff member to swipe and collect printed material is not allowed. When task(s) completed photocopier/printer must be checked to ensure no personal data is left behind. Printers are not allowed in individual offices unless directed by the CEO.

22.0 Fax Machines

22.1 Personal data should not be sent or received via fax. Staff shall use the authorised health mail accounts which have been allocated for the disability and palliative care services.

23.0 Photographs/Video Images

23.1 Written consent must be sought for publication/public use of photographs/videos taken of the children/adults, and the publication must be approved from the Line Manager before going live.

23.2 Written consent is not required for photos/videos of children/adults' holidays, parties, outings and activities which remain within the organisation unless a parent specifically states otherwise.

23.3 Photos/Video must not be downloaded to any personal computer unless that personal computer belongs to a service user and is done with the child/adult's consent.

23.4 Photographs/Video cameras and tapes must be stored securely in the relevant area and images must be deleted/destroyed when no longer required.

23.5 Where volunteers/external photographers are required for events within the service they are required to complete a disclaimer confirming

- All ownership of the photographs remain the property of LauraLynn
- To upload all photographs (in all formats) to the designated file sharing folder.
- Once all photographs have been uploaded to the designated file sharing folder they will delete them from all of their devices
- Will not to keep any photographs (in any format) for any use either for that event or in the future

24.0 Mobile Phones

24.1 Only authorised staff are permitted to use the camera facility on a mobile phone to take photographs/videos of children/adults. No other member of staff shall use their personal mobile phone to take photographs unless that mobile phone belongs to a child/adult and is done with the childs/young person's consent.

24.2 Covert recording of conversations in the workplace is strictly forbidden.

24.3 Personal data regarding children/adults or staff members must not be sent via text messaging. (See Code of Conduct for Staff Policy).

25.0 Children/Adults Information

25.1 All children/adults that are currently availing of services, their files are kept in the relevant house. Respite children who are availing of the service on an ad hoc basis, their files are brought over to the relevant house where the child is located, when these children are not availing of the service, their files are kept in the file room in LauraLynn House and/or in the file room in Littleoak area. Access to these areas are controlled, i.e. fob in and out.

25.2 Retrieval of the children/adults files are restricted to Managers, Nurses, and Administrative Staff.

25.3 If a file is being removed from an area for updating, staff must inform the Manager and return the file as soon as practicable.

25.4 Separate box files are held in respect of all children/adults and these are used to store older documentation that is on file, which means that the main file does not become overloaded with data and is easy to maintain and current documentation is easy to view. These files are stored in the file rooms in LauraLynn and Littleoak. Access to these areas are controlled, i.e. fob in and out.

25.5 Files of children/adults who are no longer with availing of the services (either deceased or transferred) as well as current older children/adults files are sent to Kefron Filestores where they are stored indefinitely, in accordance with Data Protection and Freedom of Information Act.

26.0 Evaluation

This policy and associated procedure will be amended as necessary to reflect any changes to best practice, law or substantial organisation changes. It is reviewed and evaluated for appropriateness and effectiveness every two years at a minimum/according to expiry and unless otherwise stated.

.

27.0 Appendices

27.1 Appendix 1: Access Request Form

27.1 Appendix 1

Data Protection Access Request Form

Request for a copy of Personal data
Data Protection Acts 1988 and 2003

Important: We may require proof of the applicant's identity (e.g. passport or driver's license) and address (e.g. utility bill) to ensure that the person making the access request is acting legitimately.

Section A – please complete this section
Full Name: _____
Postal Address: _____
_____
Telephone / email: _____ _____
*we may need to contact you to discuss your Access Request

Section B – please complete this section
I, _____ (insert name) wish to have access to data that I believe the Service retains on me as outlined below (please include the name of service(s) and any other relevant details to your access request)
_____
_____
_____
_____
Signed: _____ Date: _____

Checklist: Have you:	Yes	No
1. Completed the Access Request Form in full?	□	□
2. Attached a photocopy of proof of your identity and address if required?	□	□
3. Signed and dated the Access Request?	□	□

Please return this form to: Data Protection Officer, LauraLynn, Ireland's Children's Hospice, the Children's Sunshine Home, Leopardstown Road, Foxrock, Dublin 18

Office Use Only:
_____
_____

If you are not satisfied with the outcome of your access request you are entitled to make a complaint to the Data Protection Commissioner who may investigate the matter for you.