Larchfield house
Dementia care specialists

Initial Privacy Impact Assessment - Policy & Procedure

Category: GDPR – Sub-category: Policies

Created: 30/04/2018	**Name:** Cliff Grand-Scrutton	**Signature:** X	**Document Owner:** A N Other

Key Question	**Key Line of Enquiry (KLOE)**
WELL-LED	**W2 – Does the governance framework ensure that responsibilities are clear, and that quality performance, risks and regulatory requirements are understood and managed?**
	W3 – How are the people who use the service, the public and staff engaged and involved?

Purpose:

The purpose of this policy is to enable Larchfield House to conduct an audit of the personal data it holds and processes to determine whether the personal data and processing comply with GDPR.

The principles set out in this policy will be explained in more detail in future policies and procedures and guidance.

This policy applies to all staff at Larchfield House who process personal data about other staff, Residents and any other living individual as part of their role.

To support Larchfield House in meeting the Key Lines of Enquiry as above.

To meet the legal requirements of the regulated activities that Larchfield House is registered to provide:

- Health and Social Care (Safety and Quality) Act 2015
- Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003
- General Data Protection Regulation 2016
- Data Protection Bill 2017

Scope:

The following roles may be affected by this policy:

- All staff

Larchfield house
Dementia care specialists

Initial Privacy Impact Assessment - Policy & Procedure

Category: GDPR – Sub-category: Policies

The following people may be affected by this policy:

- Residents

The following stakeholders may be affected by this policy:

- Commissioners

Objectives:

The objective of this policy is to enable Larchfield House to determine whether its processing of personal data complies with GDPR.

Larchfield House will use this policy to conduct an assessment of its personal data and, if necessary following the assessment, Larchfield House will delete or destroy the personal data it holds and/or change the way in which it processes the personal data.

This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.

To ensure that Larchfield House complies with the Records Management Code of Practice for Health and Social Care 2016 and the detailed Retention Schedules and doesn't destroy any relevant personal data.

Policy:

Larchfield House recognises that a Privacy Impact Assessment (IPA) is essentially a **risk assessment** of proposed processing of personal data. Larchfield House understands that if Larchfield House is processing personal data that is likely to result in a **high risk** to the Data Subject's rights, a PIA must be carried out prior to commencing that processing.

An effective PIA will allow Larchfield House to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur. The purpose of this initial Privacy Impact Assessment which forms part of this documentation is to clarify what personal data is currently held, where, how and by whom, by including organisations that may hold or collect personal data for Larchfield House.

Larchfield House will work with staff members identified by the Data Protection Officer, with partner organisations and, where appropriate, with the Residents affected to identify and reduce privacy risks in order to undertake an initial Privacy Impact Assessment. Once the information has been gathered, the responses will be considered by Larchfield House alongside the key principles of GDPR (which will be described in more detail in the relevant guidance note).

Larchfield house
Dementia care specialists

Initial Privacy Impact Assessment - Policy & Procedure
Category: GDPR – Sub-category: Policies

Key Considerations

Once the initial Privacy Impact Assessment has been completed, Larchfield House will review the key considerations outlined in the procedure and take action where required.

Procedure:

Circulate the initial Privacy Impact Assessment Form to all key members of staff for completion.

Circulate all relevant guidance, particularly guidance in respect of GDPR – Key Principles, to all key staff members to assist completion of the Initial Privacy Impact Assessment.

Form Completion – Types of Personal Data

Explanatory Comment

- The form is drafted on the basis that a separate form will be used for each type of personal data. Examples of types of personal data include 'name', 'email address', 'postal address', 'phone number', 'medical records', 'health records', 'Care Plan', 'next of kin information', 'recruitment records', 'bank details', 'staff management records' or 'CCTV'. These are examples, and Larchfield House may have other types of personal data that are being held for purposes other than listed. The forms should not refer specifically to an individual (for example, "Joe Bloggs" or "joe.bloggs@gmail.com").
- The intention is that a form will be completed for each type of personal data. It is possible that more than one form for the same type of personal data may be completed dependent upon the scope and knowledge of the person nominated by Larchfield House to complete the form. Each member of staff only needs to complete a form for the types of personal data they process – if a member of staff does not use Care Plans, they do not need to complete a form for Care Plans, for example.
- Larchfield House may review documents that include personal data such as complaints, the visitors book, safeguarding records, marketing records, Resident family, relatives and friends' details. However, the type of personal data is not the document itself, it is the personal data within the document. For example, if a complaint is reviewed, it is not the complaint that is the personal data, it is the name, address or other details that identify individuals within it.
- Larchfield House may find that the same response applies to several types of personal data. For example, the retention periods for medical records, health records and Care Plans may be the same. It is for this reason that Larchfield

House may choose to incorporate the questions from the form into a spreadsheet, listing the types of personal data in the left-hand column. This would enable Larchfield House and its members of staff to easily duplicate responses for all the questions and would result in one single spreadsheet being produced by each key member of staff/team rather than multiple copies of the form.

Question 1 of the Form – "How did you obtain the personal data?"

Explanatory Comment

- Was the personal data (i.e. the email address, medical record, Care Plan) obtained directly from the Resident or from a third party, such as the Resident's carer, next of kin or medical provider?

Question 2 – "Did you get consent to collect their personal data"

Explanatory Comment

- When the personal data was obtained, did you get express consent from the Data Subject (for example, the Resident or member of staff) to process that personal data?
- Larchfield House may have other grounds for processing the personal data (which will be explained in a guidance note) but it is a useful starting point to understand if consent has been obtained or not.

Question 3 – "If you did not get consent, on which ground are you processing the personal data?"

Explanatory Comment

- Can you reply on legitimate interest or fulfilment of a contract or, in the case of Special Categories of Data, is the personal data being processed in the field of employment or for the provision of health and social care services?
- These terms will be explained in more detail in future guidance notes.

Question 4 – "Why do you need the personal data"

Explanatory Comment

- Do you use the personal data for HR/staff purposes such as payroll or general employment purposes?
- Do you use the personal data to be able to provide care to a Resident? Do you have the personal data simply because it may be useful in the future?

Larchfield house
Dementia care specialists

Initial Privacy Impact Assessment - Policy & Procedure
Category: GDPR – Sub-category: Policies

Question 5 – "Is the personal data still relevant"

Explanatory Comment

- Do you still use the personal data?
- Do you have any personal data for former members of staff, or for Residents for whom you no longer provide care?

Question 6 – "Do you destroy or delete personal data you no longer need?"

Explanatory Comment

- Do you shred hard copies or permanently erase online documents?
- If not, what do you do with the personal data when you no longer need it?

Question 7 – "Do you make sure that the personal data is kept accurate and up to date?"

Explanatory Comment

- Do you have processes in place for regularly checking and updating details with staff and Residents?

Question 8 – "What do you do with personal data that is no longer up to date?"

Explanatory Comment

- Do you retain it in the same location, do you move it to archive, do you update and replace it?

Question 9 – "Are there restrictions in place around who can access and use the personal data, and what are they?"

Explanatory Comment

- Is the personal data password protected if it is stored online?
- Is knowledge of the password restricted to only the people that need to know the information?
- Are there other technical/IT security measures in place?
- Are hard copies of personal data stored in locked filing cabinets?
- Is access to the filing cabinets limited to only those who need access to the information?

- Are there other security measures in place?

Question 10 – "How long do you keep personal data?"

Explanatory Comment

- What do you do with the personal data when a member of staff leaves or when care is no longer being provided to a particular Resident?
- Do you have policies and procedures in place to deal with the retention of personal data and to ensure personal data is destroyed or deleted when it is no longer needed?

Question 11 – "Do you need to keep the personal data for that long?"

Explanatory Comment

- Based on your responses to Question 10, are there statutory, business or other legitimate reasons as to why you retain the personal data for the period you have set out?

Question 12 – "Do you pass personal data to any third parties? If so, who and why?"

Explanatory Comment

- Do you pass the personal data to other service providers, to medical providers, to third parties for hosting in a data centre, or to anybody else?

Question 13 – "If you pass personal data to a third party, do you have an agreement in place with them about how they will use that personal data?"

Explanatory Comment

- Is there a written agreement in place that sets out how the third party will process and protect the personal data, and the basis on which the personal data is being transferred?"

Key Considerations
The following issues will be considered by Larchfield House following completion of the Initial Privacy Impact Assessment:

Larchfield house
Dementia care specialists

Initial Privacy Impact Assessment - Policy & Procedure
Category: GDPR – Sub-category: Policies

- **Question 1** – If the personal data was not obtained directly for the Data Subject, do grounds exist to justify the collection of that personal date i.e. legitimate interests or fulfilment of a contract (see future guidance note for more information)? If Larchfield House sends marketing communications, it will consider whether it has obtained consent (if necessary) and whether its marketing communications comply with GDPR and PECR (Privacy and Electronic Communication Regulations)
- **Question 2** – If yes, consider whether consent is the appropriate ground to rely on going forwards for collection of that type of personal data
- **Question 3** – If consent was not obtained from the Data Subject to process the personal data, Larchfield House will consider whether it is able to rely on another ground (such as legitimate interest or, if the personal data are Special Categories of Data, is the processing necessary for the provision of health and social care or treatment, or as part of the employment of the member of staff)? These principles will be explained in more detail in the guidance entitled GDPR – Key Principles. If Larchfield House as no ground for processing the personal data, continuing to process it may result in a breach of GDPR
- **Question 4** – If Larchfield House does not have a particular need for the personal data, it will consider deleting the personal data and ceasing collection of it. Failure to do so may result in a breach of GDPR
- **Question 5** – If the Personal Data is no longer relevant, Larchfield House will consider deleting the personal data and ceasing collection of it. Failure to do so may result in a breach of GDPR
- **Question 6** – If Larchfield House does not currently destroy or delete personal data it no longer needs, it will consider adopting new processes to ensure that the personal data is destroyed or deleted. Failure to do so may result in a breach of GDPR
- **Question 7** – If Larchfield House does not ensure that personal data is kept accurate and up to date, it will consider adopting processes to ensure the personal data is up to date and correct. Failure to do so may result in a breach of GDPR
- **Question 8** – See above
- **Question 9** – If personal data is accessible by individuals who do not need to see the information, Larchfield House will consider adopting processes to ensure access to the personal data is restricted. Failure to do so may result in a breach of GDPR
- **Questions 10 and 11** – Personal data should only be kept during the period it is needed. Larchfield House will consider adopting processes to ensure it has appropriate retention policies in place. Failure to adopt appropriate retention policies and processes may result in a breach of GDPR
- **Questions 12 and 13** – If personal data is passed to third parties, Larchfield House will consider whether it has appropriate grounds for transferring the personal data (for example, consent, legitimate interests or fulfilment of a

contract). Ideally, data processing agreements will be entered into by Larchfield House and the third party. If the third party is located outside the EEA, Larchfield House will consider seeking legal advice to ensure the transfer is GDPR compliant

Action Plan
The form includes an action plan (in the section entitled "Results of Initial Privacy Impact Assessment"). Larchfield House acknowledges that, in some circumstances, it may be difficult for each key member of staff who has completed the form to input into the action plan.

Each member of staff who completes the form should incorporate as much information as possible in the action plan and provide any suggestions they feel are relevant or may be helpful.

Larchfield House will ensure its Data Protection Office, Privacy Officer or other nominated individual has responsibility for producing a final action plan.

Larchfield House will incorporate the action plan into its ongoing risk register for GDPR compliance.

Definitions:

Data Subject
The individual about whom Larchfield House has collected personal data.

GDPR
The General Data Protection Regulation 2016. It will replace the Data Protection Act 1998 from 25 May 2018 as the law that governs data protection in the UK. It will come into force in the UK via the Data Protection Bill.

Personal Data
Any information about a living person including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV and Special Categories of Data, defined below.

Process or Processing
Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data – at the point you collect it, you are processing it.

Larchfield house
Dementia care specialists

Initial Privacy Impact Assessment - Policy & Procedure
Category: GDPR – Sub-category: Policies

Special Categories of Data
Has an equivalent meaning to "Sensitive Personal Data" under the Data Protection Act 1998. Special Categories of Data include but are not limited to medical and health records (including care plans and information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation and political views.

ICO
The Information Commissioner's Office, a regulator which advises on and oversees compliance with GDPR

PECR
The Privacy and Electronic Communication Regulations, which sit alongside the Data Protection Act 1998 and GDPR. PECR is in the process of being updated.

Key Facts – Professionals
Professionals providing this service should be aware of the following:

- An Initial Privacy Impact Assessment should be carried out to ensure Larchfield House complies with GDPR when it processes personal data
- Penalties for non-compliance with GDPR could be significant
- Completion of an initial Privacy Impact Assessment and taking appropriate steps based on the results of the assessment will not only reduce the risk if ICO enforcement or fines but will also promote a better-quality service for Residents and an improved working environment for staff

Key Facts – People Affected by The Service
People affected by this service should be aware of the following:

- If you are a member of staff of Larchfield House, you should assist Larchfield House with completion of the Initial Privacy Impact Assessment
- Personal data held by Larchfield House about members of staff, Residents and other individuals will be processed and protected in line with GDPR

Initial Privacy Impact Assessment - Policy & Procedure
Category: GDPR – Sub-category: Policies

Outstanding Practice:

To be outstanding in this policy area you could provide evidence that:

- All key members of staff have completed the Initial Privacy Impact Assessment by the end of February 2018
- Larchfield House has deleted or destroyed all personal data it no longer needs (based on the results of the Initial Privacy Impact Assessment) by 24 May 2018
- Larchfield House has implemented new policies and processes to ensure its processing activities and personal data it holds are compliant with GDPR and such policies and processes will take effect on or before 24 May 2018
- Larchfield House has implemented processes so that lessons are learned when there are data security breaches

Initial Privacy Impact Assessment - Policy & Procedure
Category: GDPR – Sub-category: Policies

Appendix:

- ***Underpinning Knowledge – What have we used to ensure that the policy is current****:*

  Information Commissioner's Office (2018) Guide to the General Data Protection Regulation (GDPR) [Online] Available from: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed: 16/01/2018]

  Information Commissioner's Office (2018) Preparing for the General Data Protection Regulation (GDPR) – 12 steps to take now. [Online] Available from: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf [Accessed: 16/01/2018]

  Intersoft Consulting (2018), Final text of GDPR. [Online] Available from: https://gdpr-info-eu/ [Accessed: 06/02/2018]

- ***Relevant Legislation:***

  Health and Social Care (Safety and Quality) Act 2015

  Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003

  General Data Protection Regulations 2016

  The Data Protection Bill 2017

Larchfield house
Dementia care specialists

Initial Privacy Impact Assessment - Policy & Procedure
Category: GDPR – Sub-category: Policies

In Summary:

The Initial Privacy Impact Assessment should be completed by organisations between now and 25 May 2018. The sooner it is completed, the more time the organisation will have to review and cleanse their personal data and implement new policies and procedures (if necessary) to ensure compliance with GDPR.

Suggested Action:

- Notify all staff of changes to policy
- Training Sessions
- Discuss in team meetings
- Discuss in supervision sessions
- Impact assessment/action plan
- Confirm relevant staff understand the content of the policy