

**Privacy Policy**

**Next planned review in 12 months, or sooner as required.**

Business Impact:	Low	Medium	High	Critical
			X	

<b>Reason for this review:</b>	New Policy – April 2018
<b>Were changes made?</b>	Yes
 <b>Summary:</b>	This Privacy Impact Assessment policy will enable organizations to determine when they need to conduct Privacy Impact Assessments. The form included in the policy should be used as a template for each Privacy Impact Assessment.
<b>Relevant Legislation:</b>	<ul style="list-style-type: none"> <li>General Data Protection Regulation 2016</li> <li>Data Protection Act 2018</li> </ul>
<b>Underpinning Knowledge - What have we used to ensure that the policy is current:</b>	<ul style="list-style-type: none"> <li>GDPR, (2018), <i>GDPR Final Text - Articles 35 and 36, Recitals 74-77, 84, 89-92, 94 and 95.</i> [Online] Available from: <a href="http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&amp;from=EN">http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&amp;from=EN</a> [Accessed: 04/05/2018]</li> </ul>
 <b>Action:</b>	<ul style="list-style-type: none"> <li>Establish process to confirm the understanding of relevant staff</li> <li>Establish training sessions for staff</li> <li>Widely distribute the 'Key Facts' of the policy</li> </ul>

# Privacy Policy

This page is deliberately left blank

# Privacy Policy

## 1. Purpose

1.1 The purpose of this policy is to provide a template privacy impact assessment ("PIA") to be used by Astoria Homecare on an ongoing basis, as necessary. This policy also explains when a PIA should be conducted.

1.2 Astoria Homecare will ensure that the Data Protection Officer will determine when a PIA is required and will complete the PIA, with input as necessary from colleagues and teams.

1.3 To support Astoria Homecare in meeting the following Key Lines of Enquiry:

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?

1.4 To meet the legal requirements of the regulated activities that Astoria Homecare is registered to provide:

- General Data Protection Regulation 2016
- Data Protection Act 2018

## 2. Scope

2.1 The following roles may be affected by this policy:

- All staff

2.2 The following people may be affected by this policy:

- Client or Service Users

2.3 The following stakeholders may be affected by this policy:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority
- NHS

## 3. Objectives

3.1 The objective of this policy is to ensure that Astoria Homecare considers the potential data protection and GDPR implications of any new processes or systems it introduces, or of any changes that impact on its processing of personal data.

3.2 By reviewing and utilising the form set out in this policy, Astoria Homecare will be able to provide evidence of the decisions it has taken and changes it has made that may impact on the processing it carries out.

# Privacy Policy



## 4. Policy

- 4.1** Astoria Homecare understands that a PIA will enable it to identify and minimise the risks of any project it wishes to carry out.
- 4.2** Astoria Homecare understands that PIAs must be conducted for specified types of processing (listed in the Procedure section below) as well as for processing that may result in a high risk for affected individuals.
- 4.3** Astoria Homecare understands that a PIA should:
- Describe the nature, scope, context and purposes of the processing
  - Assess whether the processing is necessary and proportionate and in compliance with GDPR
  - Identify and assess risks to affected Data Subjects; and
  - Identify the measures it will take to mitigate those risks
- 4.4** Astoria Homecare understands that if a PIA identifies that processing may be high risk and it is unable to take steps to mitigate those risks, it should notify the ICO and seek advice from the ICO as to whether it should carry out the processing.

# Privacy Policy

## ●→ 5. Procedure

**5.1** Astoria Homecare will implement a process for deciding whether a PIA is necessary and, if so, the steps that it will take to conduct the PIA. Astoria Homecare will use the form attached to this policy when conducting a PIA.

**5.2** Astoria Homecare will provide training to its employees about when a PIA is necessary and how to conduct a PIA.

**5.3** Astoria Homecare will conduct PIAs in the following scenarios:

- Where Astoria Homecare intends to use systematic and extensive profiling or automated decision-making to make significant decisions about Data Subjects
- Where personal data relating to children will be processed for profiling or automated decision making, for marketing to offer online services directly to the children
- Where Astoria Homecare will process special categories of data or criminal offence data on a large scale
- Where Astoria Homecare intends to monitor a publicly accessible place on a large scale
- Where new technologies are introduced by Astoria Homecare that may impact on its processing activities
- Where Astoria Homecare intends to process biometric or genetic data
- Where Astoria Homecare intends to combine, compare or match personal data from multiple sources
- Where Astoria Homecare processes personal data without providing a privacy policy directly to the affected Data Subject
- Where the processing will involve tracking individuals' behaviour (whether online or offline)
- Where the processing could result in a physical harm if there is a breach of security

**5.4** Astoria Homecare will consider carrying out PIAs in the following circumstances, as well as in any other circumstances which Astoria Homecare considers to be potentially high risk:

- Where Astoria Homecare processes special categories of data or personal data of a highly personal nature
- Where Astoria Homecare conducts large-scale processing; and
- Where the processing concerns vulnerable Data Subjects

Astoria Homecare acknowledges that because of the types of services it provides, it may need to conduct PIAs on a regular basis to ensure that Data Subjects, including Client or Service Users, are protected.

**5.5** Astoria Homecare will also conduct a PIA if the nature or purpose of the processing it carries out changes.

**5.6** Astoria Homecare will document the steps taken as part of the PIA and the outcomes in line with the form attached to this policy.

**5.7** Astoria Homecare will take any steps it identifies as being necessary to mitigate risks associated with the processing and will document the steps taken and the outcome of those steps.

# Privacy Policy

- → 5. Procedure
- →  6. Definitions

## 6.1 Data Subject

- The individual about whom Astoria Homecare has collected personal data

## 6.2 Data Protection Act 2018

- The Data Protection Act 2018 is a United Kingdom Act of Parliament that updates data protection laws in the UK. It sits alongside the General Data Protection Regulation and implements the EU's Law Enforcement Directive

## 6.3 GDPR

- **General Data Protection Regulation (GDPR)** (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It was adopted on 14 April 2016 and after a two- year transition period became enforceable on 25 May 2018

## 6.4 ICO

- The Information Commissioner's Office

## 6.5 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

## 6.6 PIA

- A Privacy Impact Assessment, also known as a Data Protection Impact Assessment

## 6.7 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

## 6.8 Special Categories of Data

- Has an equivalent meaning to "Sensitive Personal Data" under the Data Protection Act 2018. Special categories of data include but are not limited to medical and health records (including 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