

Privacy Notice Policy & Procedure







Policy Review Sheet

Review Date: 23/05/18 **Policy Last Amended:** 23/05/18

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

Note: The full policy change history is available in your online management system.

Business Impact:	Low	Medium	High	Critical
			X	
These changes require action as soon as possible. Changes include fixed implementation dates which are detailed within the policy.				

 Reason for this review:	New Policy
 Were changes made?	Yes
 Summary:	This Privacy Impact Assessment policy will enable organisations 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.
 Relevant Legislation:	<ul style="list-style-type: none"> General Data Protection Regulation 2016 Data Protection Act 2018
 Underpinning Knowledge - What have we used to ensure that the policy is current:	<ul style="list-style-type: none"> GDPR, (2018), <i>GDPR Final Text - Articles 35 and 36, Recitals 74-77, 84, 89-92, 94 and 95.</i> [Online] Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Accessed: 04/05/2018]
 Suggested action:	<ul style="list-style-type: none"> Encourage sharing the policy through the use of the QCS App Establish process to confirm the understanding of relevant staff Establish training sessions for staff Widely distribute the 'Key Facts' of the policy

Privacy Notice Policy & Procedure

This page is deliberately left blank

Privacy Notice Policy & Procedure

1. Purpose

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

1.2 Caring Direct Ltd will ensure that the will determine when a PIA is required and will complete the PIA, with input as necessary from colleagues and teams.

1.3 To support Caring Direct Ltd 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 Caring Direct Ltd 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:

- 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 Caring Direct Ltd 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, Caring Direct Ltd 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 Notice Policy & Procedure



4. Policy

4.1 Caring Direct Ltd understands that a PIA will enable it to identify and minimise the risks of any project it wishes to carry out.

4.2 Caring Direct Ltd 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 Caring Direct Ltd 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 Caring Direct Ltd 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.



5. Procedure

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

5.2 Caring Direct Ltd will provide training to its employees about when a PIA is necessary and how to conduct a PIA.

5.3 Caring Direct Ltd will conduct PIAs in the following scenarios:

- Where Caring Direct Ltd 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 Caring Direct Ltd will process special categories of data or criminal offence data on a large scale
- Where Caring Direct Ltd intends to monitor a publicly accessible place on a large scale
- Where new technologies are introduced by Caring Direct Ltd that may impact on its processing activities
- Where Caring Direct Ltd intends to process biometric or genetic data
- Where Caring Direct Ltd intends to combine, compare or match personal data from multiple sources
- Where Caring Direct Ltd 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 Caring Direct Ltd will consider carrying out PIAs in the following circumstances, as well as in any other circumstances which Caring Direct Ltd considers to be potentially high risk:

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

Caring Direct Ltd 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 Service Users, are protected.

5.5 Caring Direct Ltd will also conduct a PIA if the nature or purpose of the processing it carries out changes.

5.6 Caring Direct Ltd will document the steps taken as part of the PIA and the outcomes in line with the form attached to this policy.

5.7 Caring Direct Ltd 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 Notice Policy & Procedure



6. Definitions

6.1 Data Subject

- The individual about whom Caring Direct Ltd has collected personal data

6.2 Data Protection Act 1998 or DPA

- The law that relates to data protection. It will remain in force until and including 24 May 2018. It will be replaced by GDPR on 25 May 2018

6.3 GDPR

- The General Data Protection Regulation 2016. It will replace the Data Protection Act 2018 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

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



Key Facts - Professionals

Professionals providing this service should be aware of the following:

- All staff should be made aware of how GDPR impacts on their role and ensure that they know who in the Caring Direct Ltd organisation has overall responsibility for data protection
- A PIA is essentially a risk assessment of proposed processing of personal data. If Caring Direct Ltd 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.
- A six-step process maps the lifecycle of the personal data in order to establish: the provenance of the data, the manner of the processing involved, the location of the processing, the relevant stakeholders and the deletion/anonymisation process

Privacy Notice Policy & Procedure



Key Facts - People Affected by The Service

People affected by this service should be aware of the following:

- PIAs will be conducted by Caring Direct Ltd to ensure that if its processing of personal data changes, any associated risks will be understood and acted upon



Further Reading

There is no further reading for this policy, but we recommend the 'Underpinning Knowledge' section of the review sheet to increase your knowledge and understanding.



Outstanding Practice

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

- You have implemented a PIA policy and all staff are aware of the potential need to conduct a PIA
- The wide understanding of the policy is enabled by proactive use of the QCS App



Forms

The following forms are included as part of this policy:

Title of form	When would the form be used?	Created by
Privacy Impact Assessment	This form should be used each time an organisation determines that it is necessary to conduct a PIA in line with the guidelines set out in this policy and procedure	QCS