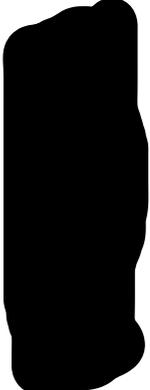


# Data Protection Assurance Checklist

Process Title:	Thorn Heys
GP Lead: (name and job title):	Norma Currie, Head of Commissioning for Learning Disabilities and Autism.
Validator's name (Information Governance):	Pippa Joyce and
Validation date:	11 <sup>th</sup> August 2021
Data Protection Officer consulted (date):	13 <sup>th</sup> August 2021
Data Protection Officer comments:	Approved
Data Protection Officer signature:	
SIRO approval (date):	
SIRO comments:	
SIRO signature:	

# OVERVIEW

What is the process under consideration?	Guidance
<p>Present a description of the process: its name, purposes, stakeholders, context of use, etc</p> <p>Thorn Heys is a service provided by Cheshire and Wirral Partnership Trust (CWP) for respite care for adults with a learning disability. This is commissioned by the CCG as part of the block contract with CWP. The service is located on the Ashton House site and has been subject to review in line with the needs of the cohort of people accessing the service and the wider provision commissioned across Wirral.</p> <p>As part of this redesign CWP are undertaking a joint needs assessment of all families that are currently accessing this service. This will determine what the individual needs are and how we can support them going forward as the current model is outdated.</p> <p>As part of this process the following is anticipated:</p> <ul style="list-style-type: none"> <li>• CWP will perform a joint needs assessment whereby an options appraisal will be performed and the aggregated results of these will be presented to the senior executives of the CCG and the Council to approve the future direction of travel for the service provided.</li> <li>• CWP and the Local Authority are the data controllers</li> <li>• The CCG are commissioners only</li> <li>• The only data that will be collected will be the joint needs assessment by CWP. No personal data will be shared with the CCG and only aggregated report finding data will be used by the CCG to determine the future of the Thorn Heys Service.</li> <li>• All data will remain the property of the Data Controllers and will stay within the Data Controller infrastructure. This will be assessed in the DPIA completed by the Data Controllers.</li> </ul>	<p>Present a brief outline of the processing under consideration, its nature, scope, context, purposes and stakeholders.</p> <p><b>Personal data</b></p> <p>Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p> <p>See <a href="#">Art. 4.1 of [GDPR]</a></p> <p><b>Pseudonymised data</b></p> <p>Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.</p> <p><b>Definition: Data Controller</b></p> <p>Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by</p>

	<p>Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. See <a href="#">Art. 4.7 of [GDPR]</a></p> <p>Definition: Data Processor</p> <p>Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, see <a href="#">Art. 4.8 of [GDPR]</a>.</p> <p>The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law, see <a href="#">Art. 29 of [GDPR]</a></p>
<p><b>Has the CCG sought suitable assurance that all protective measures are in place from the Data Controller?</b></p>	
<p><b>Please answer Yes or No</b></p>	
<p>The CCG has explained to CWP that they must undertake a DPIA and a DSA must be completed between Data Controllers for this project.</p>	
<p><b>What governance measures are in place to oversee the confidentiality, security and appropriate use of the data?</b></p>	
<p><b>we need confirmation that each organisation who will have access to PCD, has a compliant toolkit, IG security policies in place, breach procedures in place and that their staff are trained. If a system is involved, it should also include all the security information around the system including where the servers are held...</b></p>	

All organisations involved in this project are required to comply with Information Governance standards in terms of training, toolkit submissions and IG policy. Each has dedicated IG teams to support the delivery of annual compliance, toolkit submission and training.

CWP (ODS RXA) are DSP Toolkit compliant as per 20/21 Standards Met

Wirral CCG (ODS 12F) are DSP Toolkit compliant as per 20/21 Standards Met

Wirral Metropolitan Borough Council (ODS 319) are DSP Toolkit compliant as per 20/21 Standards Met