Appendix 2C to the Connection Agreement

Data protection relationship between Connecting Party and End User Organisation(s)

The terms set out in this Appendix 2C shall apply in relation to Processing carried out by the Connecting Party pursuant to its provision of its products and services to End User Organisations and Individual End Users.

1. In this Appendix:

   "Controller", "Data Subject", "Processor", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the meanings set out in the Data Protection Laws and **"Process"** shall be construed in accordance with the definition of **"Processing"**;

   "Caldicott Principles" means the six principles developed by Dame Fiona Caldicott for appropriate use of patient information, as amended from time to time;

   "Data Protection Laws" means applicable legislation protecting the fundamental rights and freedoms of individuals, in respect of their right to privacy and the processing of their personal data, as amended from time to time, including 'the General Data Protection Regulation' (**"GDPR"**) and the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, together with decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, Supervisory Authorities and other applicable government authorities;

   "Data Security and Protection Toolkit" means the online self assessment tool and guidance managed by NHS Digital which reflects the National Data Guardian for Health and Care's data security standards, and enables organisations to measure their performance against such standards;

   "ICO" means the UK's Information Commissioner's Office;

   "NHS Constitution" means the NHS Constitution for England as amended from time to time;

   "Restricted Country" means any country other than the United Kingdom.

2. Where acting as a Processor on behalf of a third party Controller, the Connecting Party shall:

   2.1 comply with its obligations as a Processor under the Data Protection Laws;

   2.2 ensure that it has entered into with the relevant Controller(s) legally binding terms governing the Processing in accordance with the requirements of Article 28(3) of the GDPR, and shall comply with such terms ("**Controller-Processor Terms**");

   2.3 not Process or otherwise transfer or permit the transfer of any Personal Data in or to any Restricted Country unless (i) this is expressly permitted by the Controller-Processor Terms; or (ii) the transfer is required by EU or member state law to which the Connecting Party is subject, and if this is the case, then the Connecting Party shall inform NHS Digital of that permission or requirement before Processing the Personal Data, unless a law prohibits such information being provided on important grounds of public interest.

3. Where acting as a Controller, the Connecting Party shall comply with its obligations as a Controller under the Data Protection Laws and with the terms of any agreement relating to its Processing of Personal Data that it has entered into with the relevant End User Organisation(s). Where the Connecting Party is acting as a joint Controller with any other organisation, the Connecting Party shall ensure that it complies with the requirements of Article 26 of the GDPR

4. Regardless of its role (Controller or Processor) in Processing any Personal Data the Connecting Party shall:

   4.1 ensure that any transfer of Personal Data to a Restricted Country (including pursuant to paragraph 2.3) is permitted under, and complies with, the requirements of, the Data Protection Laws;

   4.2 ensure it has robust business continuity management plans and supporting procedures;

   4.3 comply (and shall procure that all its contractors, subprocessors and agents comply) with the Data Security Protection Toolkit; abide by the Caldicott Principles; and not do anything which would cause NHS Digital or the End User Organisation to be in breach of the NHS Code or the NHS Constitution;.

   4.4 comply with the DSP Toolkit incident reporting requirements in respect of, and notify NHS Digital of, any Personal Data Breach affecting the Personal Data as soon as the Connecting Party discovers such Personal Data Breach and provide such information and cooperation as may be required;

   4.5 comply with its obligations under the Network and Information Systems Regulations 2018 to the extent applicable to its performance of this Connection Agreement or provision of the relevant products or services;

   4.6 comply (and shall procure that all its contractors and subcontractors) comply with NHS Digital's cyber security guidance and policy (where available) as set out on the NHS Digital web site;

4.7 indemnify NHS Digital, and keep NHS Digital indemnified, against damages, costs, claims, demands, expenses, professional costs, charges and/or monetary penalty notices arising from enforcement by a Supervisory Authority and/or assertion of rights by Data Subjects, arising from a breach by the Connecting Party of the Data Protection Laws and/or the data processing provisions set out in this Connection Agreement.

5. Should a Service require identity verification of an Individual End User the Connecting Party shall comply with the Identity Verification and Authentication Standards for Health and Care as set out or linked to on a Services Web Page.

6. The parties agree to take account of any guidance issued by a Supervisory Authority.

7. The Connecting Party warrants that it has and its agents and employees have the necessary legal authority in any country where any Processing of Personal Data is authorised to take place under this Connection Agreement, the Controller-Processor Terms and/or any agreement of the kind referred to in paragraph 3, and undertakes to comply with any of the Data Protection Laws which is applicable in such country.