LEEDS CITY COUNCIL

DATA PROCESSING AGREEMENT

THIS AGREEMENT is made the day of

Between

1 The Parties

1.1 Leeds City Council, (herein after called the "Data Controller") of Civic Hall, Calverley Street, Leeds, LS1 1UR of the one part and

NHS Leeds of North West House, West Park Ring Road, Leeds, LS16 6QG (herein after called the "Data Processor") of the other part.

1.2 NHS Leeds shall act as Data Processor for the purposes described in this Agreement. Leeds City Council and NHS Leeds shall then act as Data Controllers in common in the transfer of Data to **Purchasing Index Ltd, 150 Buckingham Palace Road, London SW1W 9TR** for the purpose of CareTrak as described in Appendix 3

2 Purpose

The key usage of this Data is for the purpose of business intelligence through CareTrak and matching Data for Risk Stratification only. It will not be used for any other purpose except when consent/permission has been sought. See Appendices:

Appendix 1 - Overview of the Integrated Health and Socal Care Data Sharing Model
Appendix 3 - Agreement for the transfer and processing of health and social care Data
Appendix 5 - Data specification for the Leeds Risk Stratification Tool and CareTrak systems

3 Definitions

The following words and phrases used in this Agreement shall have the following meanings except where the context otherwise requires:

3.1 The expressions "Data", "Data Controller", "Data Processor", "Personal Data", "Sensitive Personal Data", "Processing", "Information Commissioner", "Data Subject Access" have the same meaning as in Sections 1, 2, and 6 of The Data Protection Act 1998, as amended by The Freedom of Information Act 2000.

3.2 "Aggregated Data" means Research Data grouped together to the extent that no living individual can be identified from that Aggregated Data or any other Data in the possession of, or likely to come into the possession of any person obtaining the Aggregated Data.

3.3 "Agreement" means this Data Processor agreement together with its Schedules and all other documents attached to or referred to as forming part of this agreement.

3.4 "Confidential Information" means any information relating to the Data Controller's customers and prospective customers, current or projected financial or trading situations, business plans, business strategies, developments and all other information relating to the Data Controller's business affairs including any trade secrets, know-how and any information of a confidential nature imparted by the Data Controller to the Data Processor during the term of this Agreement or coming into existence as a result of the Data Processor's obligations, whether existing in hard copy form or otherwise, and whether disclosed orally or in writing. This definition shall include all Personal Data.

3.5 "Services" means the services to be provided by the Data Processor during the term of this Agreement, as described in Appendix 6 -- Protocols for managing access permissions within the CareTrak and Leeds Risk Stratification Tools

3.6 Headings are inserted for convenience only and shall not affect the construction or interpretation of this Agreement and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Agreement;

3.7 Any reference to any enactment or statutory provision shall be deemed to include a reference to such enactment or statute as extended, re-enacted, consolidated, implemented or amended and to any subordinate legislation made under it; and

3.8 The word 'including' shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word 'include' and its derivatives shall be construed accordingly.

4 Information provision

4.1 The Data will be provided over a set time period to be agreed in advance by both Parties as identified in the schedule attached at Appendix 5 - Data specification for the Leeds Risk Stratification Tool and CareTrak systems

4.2 This agreement is made for one year and optionally may be extended for a further year, if agreed by all parties. The Data will be shared on a monthly basis

Ownership of the Data shall at all times remain with the Data Controller.

5 Use, Disclosure and Publication

5.1 The Data will be used exclusively for CareTrak and Risk Stratification (as described in Appendix 6) and will NOT be matched with any other Personal Data otherwise obtained from the Data Controller, or any other source, unless specifically authorised in writing by the Data Controller.

5.2 The Data will NOT be disclosed to any third party without the written authority of the Data Controller except as in accordance with paragraph 1.2 above.

5.3 Access to the Data will be restricted to those employees of the Data Processor, NHS Leeds Information Systems and Delivery Team as listed below and approved by the Data Controller, directly involved in the processing of the Data in pursuance of the Purpose.

5.3.1 Senior Information Manager – Chris Cooper; Information manager (x 3); Information officer (x 2)

5.4 Data analysis through CareTrak will be licensed to NHS Leeds Chief Information officer's Department

5.5 The Data will be used solely for the Purpose and may be published at aggregate level taking account of small numbers, see ONS guidance (Appendix 6)

5.6 No steps will be taken by the Data Processor for CareTrak or Risk Stratification to contact any Data Subject identified in the Data.

5.7 Personal Data used for research will not be published in identifiable form unless the persons concerned have given their consent and in conformity with other safeguards laid down by domestic law.

6 Data Protection and Human Rights

6.1 Martin Foster, Information Compliance Officer, Adult Social Care, Leeds City Council. David Green, Information Governance and Records Manager, NHS Leeds, will be responsible for any Data Protection or Human Rights issues that might arise

6.2 The use and disclosure of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Agreement by the Data Protection Act 1998 and the Human Rights Act 1998. All relevant codes of practice or data protection operating rules adopted by the Parties will also reflect the data protection practices of each of the parties to this Agreement.

6.3 The Parties agree and declare that the information accessed pursuant to this Agreement will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the provision of information is proportional, having regard to the purposes of the Agreement and the steps taken in respect of maintaining a high degree of security and confidentiality.

6.4 The Parties undertake to comply with the provisions of the Data Protection Act 1998 and to notify as required any particulars as may be required to the Information Commissioner.

6.5 The receipt by the Data Processor from any Data Subject of a request to access to the Data covered by this Agreement must be reported immediately to the person nominated below representing the Data Controller, who will arrange the relevant response to that request.

6.6 If any Party receives a request under the subject access provisions of the Data Protection Act 1998 and Personal Data is identified as belonging to another Party, the receiving Party will contact the other Party to determine if the latter wishes to claim an exemption under the provisions of the Act.

6.7 It is acknowledged that where a Data Controller cannot comply with a request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request, unless;

(a) the other individual has consented to the disclosure of the information to the person making the request; or

(b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular, to:

- any duty of confidentiality owed to the other individual;
- any steps taken by the Data Controller with a view to seeking consent of the other individual;
- whether the other individual is capable of giving consent;
- any express refusal of consent by the other individual.

If any Party receives a request for information under the provisions of the Freedom of Information Act 2000 identified as belonging to another Party, the receiving Party will contact the other Party to determine whether the latter wishes to claim an exemption under the provisions of that Act.

6.8 Where the Data Processor receives a request for information under the provisions of the Freedom of Information Act 2000 in respect of information provided by or relating to the Data Controller, the Data Processor will contact

the person nominated below to ascertain whether the Data Controller wishes to claim any exemption including the determination of whether or not the Data Controller wishes to issue a response neither to confirm nor deny that information is held.

6.9 Where any Party receives a Notice under Section 10 of the Data Protection Act 1998, that Party will contact the person nominated below to ascertain whether or not to comply with that Notice.

6.10 The following personnel are authorised by the Parties to assume responsibility for data protection compliance, notification, security, confidentiality, audit and co-ordination of subject rights and Freedom of Information:

6.10.1 Nominated Post holders:

- **For Leeds City Council Adult Social Care:**

  Martin Foster; Information Compliance Officer

  Michele Tynan; Caldicott Guardian

- **For NHS Leeds:**

  David Green; Information Governance and Record Manager

  Dr Damian Riley; Caldicott Guardian

6.11 On reasonable notice, periodic checks may be conducted by the Data Controller to confirm compliance with this Agreement.

6.12 The Data Processor shall give reasonable assistance as is necessary to the Data Controller in order to enable him to:

- Comply with request for subject access from the Data Subjects;
- Respond to Information Notices served upon him by the Information Commissioner;
- Respond to complaints from Data Subjects;
- Investigate any breach or alleged breach of the Act.

in accordance with his statutory obligations under the Data Protection Act 1998.

7 Confidentiality

7.1 Except as specified in paragraph 1.2 above, the Data Processor shall not use or divulge or communicate to any person (other than those whose province it is to know the same for the Purpose, or without the prior written authority of the Data Controller) any Data obtained from the Data Controller, which it shall treat as private and confidential and safeguard accordingly.

7.2 The Data Processor shall ensure that any individuals involved in the Purpose and to whom Data is disclosed under this Agreement are aware of their responsibilities in connection with the use of that Data.

7.3 For the avoidance of doubt, the obligations or the confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

7.4 Respect for the privacy of individuals will be afforded at all stages of the Purpose.

7.5 Paragraph 7.1 above shall not apply where disclosure of the Data is ordered by a Court of competent jurisdiction, or subject to any exemption under the Act, where disclosure is required by a law enforcement agency or regulatory body or authority, or is required for the purposes of legal proceedings, in which case the Data Processor shall immediately notify the Data Controller in writing of any such requirement for disclosure of the Data in order to allow the Data Controller to make representations to the person or body making the requirement.

7.6 The restrictions above shall cease to apply to any Data which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Agreement.

8 Retention, Review and Deletion.

8.1 Records will not be kept longer than necessary. They will be retained for 7 years and then destroyed in line with the Data Processors 'Record Retention & Destruction Policy. Details of how long records should be kept are outlined in the NHS Code of Practice: Records Management **http://www.dh.gov.uk/en/Policyandguidance/Organisationpolicy/Recordsmanagement/index.htm**

8.2 The data processor will ensure that all records are destroyed in line with NHS standards as outlined in the 'Record Retention & Destruction' policy (see 8.1)

8.3 Alistair Cartwright, Chief Information Officer, NHS Leeds is responsible for the retention, review and deletion of the Data

9 Security

9.1 The Data Processor is level 2 compliant as recognised by the NHS Information Governance Toolkit, showing that the organisation meets the required secuity standards

9.2 The processing of Data will take place at the Data Warehouse based at: North West House. When this building is closed the Data Warehouse will move to Yeadon health centre.

9.3 Julie Oxley, Head of Information Management & Technology for Adult Social Care at Leeds City Council, is responsible for the security on behalf of the Data Controller. Alastair Cartwright, Chief Information Officer, NHS Leeds, is responsible for the security on behalf of the Data Processor

9.4 Information will be transferred to the Data Processor via the local secure network connection with health.

9.5 The Data will be encrypted along the secure network

9.6 Archived Data will be securely managed in the NHS Leeds Data Warehouse and is automatically backed up on a daily basis across 2 sites.

9.7 The Data Processor will not need to visit council premises or require access to any other council assets

9.8 The processed Data will be securely transferred via a secure FTP link to Purchasing Index Ltd by NHS Leeds on behalf of Leeds City Council. Full details of the security standards used by Purchasing Index Ltd are provided in Appendix 9.

9.9 Any security breaches will be reported immediately to Leeds City Council. Sufficient information will be supplied to meet Leeds City Council recording and reporting standards to be compliant with NHS IG Tookit requirements

9.10 The Data Processor recognises that the Data Controller has obligations relating to the security of Data in his control under the Data Protection Act 1998. The Data Processor will continue to apply those relevant obligations as detailed below on behalf of the Data Controller during the term of this Agreement.

9.11 The Data Processor agrees to apply appropriate security measures, commensurate with the requirements of principle 7 of the Data Protection Act 1998 to the Data, which states that: "appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data". In particular, the Data Processor shall ensure that measures are in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport
- deter deliberate compromise or opportunist attack, and
- promote discretion in order to avoid unauthorised access

9.12 During the term of this Agreement, Julie Oxley, Head of Information Management & Technology shall ensure that checks are carried out as necessary to ensure that the above arrangements are not compromised. There will be a review after three months of how the process is operating.

9.13 The Data Processor will ensure that the Personal Data accessed is not used other than as identified within this agreement, and that the agreement is complied with.

9.14 The Data Controller reserves the right to undertake a review of security provided by any Data Processor and may request reasonable access during normal working hours to the Data Processor premises for this purpose. Failure to provide sufficient guarantees in respect of adequate security measures will result in the termination of this Agreement.

9.15 Access to the Data will be confined to authorised persons only. These will be the individual identified in the documentation attached at paragraph 5.3.1

9.16 The Data Processor undertakes not to use the services of any sub-contractors in connection with the processing of the Data without the prior written approval of the Data Controller, except those specified in paragraph 2.1

10 Indemnity

10.1 In consideration of the provision of the Data for the Purpose the Data Processor undertakes to indemnify and keep indemnified the Data Controller against any liability, which may be incurred by the Data Controller as a result of the Data Processor's breach of this Agreement.

Provided that this indemnity shall not apply:

(a) where the liability arises from information supplied by the Data Controller which is shown to have been incomplete or incorrect, unless the Data Controller establishes that the error did not result from any wilful wrongdoing or negligence on his part

(b) unless the Data Controller notifies the Data Processor as soon as possible of any action, claim or demand to which this indemnity applies, commits the Data Processor to deal with the action, claim or demand by settlement or

otherwise and renders the Data Processor all reasonable assistance in so dealing;

(c) to the extent that the Data Controller makes any admission which may be prejudicial to the defence of the action, claim or demand.

11 Disputes

11.1 In the event of any dispute or difference arising between the Parties out of this Agreement, the persons appointed pursuant to clause 9.3 of this Agreement shall meet in an effort to resolve the dispute or difference in good faith.

11.2 The Parties will, with the help of the Centre for Effective Dispute Resolution, seek to resolve disputes between them by alternative dispute resolution. If the Parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the Parties shall be at liberty to commence litigation.

12 Term, Termination and Variation

12.1 The Agreement will last for one year from the signing of this Agreement, with an option for an extension following an annual review.

12.2 The Data Controller may at any time by notice in writing terminate this Agreement forthwith if the Data Processor is in material breach of any obligation under this Agreement.

12.3 Either Party may terminate this Agreement by giving 30 days notice in writing to the other Party.

12.4 The Data Controller will have the final decision on any proposed variation to this Agreement. No variation of the Agreement shall be effective unless it is contained in a written instrument signed by both Parties and annexed to this Agreement.

13 Conclusion

13.1 This Agreement acts in fulfilment of part of the responsibilities of the Data Controller as required by paragraphs 11 and 12 of Schedule 1, Part II of the Data Protection Act 1998.

13.2 This Agreement constitutes the entire agreement between the Parties as regards the subject matter hereof and supersedes all prior oral or written agreements regarding such subject matter.

13.3 If any provision of this Agreement is held by a Court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the remaining provisions of this Agreement, which shall remain in full force and effect.

13.4 The validity, construction and interpretation of the Agreement and any determination of the performance which it requires shall be governed by the

Laws of England and the Parties hereby submit to the exclusive jurisdiction of the English Courts.

.....

Signed on behalf of Leeds City Council

.....

Date: .....

In the presence of.....

Signed on behalf of NHS Leeds

.....

Date: .....

In the presence of .....