Controller and Processor Contracts – Checklist

The Trust will use this checklist to assess our existing contracts to ensure that they will meet the requirements of the UK GDPR.

Our contracts include the following compulsory details:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Our contracts include the following compulsory terms:

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the UK GDPR;
- the processor must assist the data controller in meeting its UK GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the UK GDPR or other data protection law of the EU or a member state.

As a matter of good practice, our contracts:

- state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the UK GDPR; and
- reflect any indemnity that has been agreed.