Confidentiality and Data Security Statement

Context

You will, in the course of your role as a Peer Reviewer, have access to confidential information relating to the performance of third party advice Organisations, their Advisers and the clients they serve. Confidentiality of results is viewed as essential to all Peer Review schemes. Without some measure of confidentiality, the trust essential for participation would not be sustainable. In taking part in peer review, organisations are exposing the quality of their work to relatively unknown outsiders. Peer Reviewers will be entrusted with this information and knowledge which shall be used only for the explicit purpose of assessing and evaluating the quality of advice evidenced within case files that are submitted for assessment. It is fundamental that, either at any time during your engagement as a Peer Reviewer, or at any time after engagement has ended, for whatever reason, you do not disclose to anyone, or use for your own benefit or for the benefit of anyone else, any confidential information.

Confidential Information Definition

Confidential information includes, without limitation:

- The identity of the Organisation you are assessing and the individuals who work for it
- The identity, detail and contents of any client file you are assessing
- The quality of advice evidenced within case files for any Organisation you are assessing and the individuals who work for it
- The outcome of any peer review assessment

If you are responsible for such information at work, you must take care not to leave it unattended and, when disposed of, must ensure that it is thoroughly shredded.

Confidentiality Agreement

Your involvement with the Peer Review Scheme means that you are agreeing to:

- Not disclose any information relating to an Organisation, Adviser and client that you are assessing to anyone other than the RE Contact Manager and Technical Expert
- Not to share your access link or passwords to the secure SharePoint Document Management system
- Not to share any assessment outcome or emerging trends relating to an Organisation or individual Adviser to anyone other than the RE Contract Manager and Technical Expert
- Ensure the security and confidentiality of all Organisational and client data, including hard copy clients files whilst they are in your care

You will be asked to sign a separate Confidentiality and Non-Disclosure Agreement - Appendix 6.

Confidentiality Good Practice

You will be required to protect all confidential information to which you have access, or otherwise acquire, from loss, misuse, alteration or unauthorized disclosure, modification or access by:

- making sure paper records are not left unattended in areas where unauthorised people may view them;
- using password protection, screensavers, automatic time-outs or other appropriate security measures to ensure no unauthorised person may access confidential information from your workstation or other device;
- appropriately disposing of confidential information in a manner that will prevent a breach of confidentiality and never discarding paper documents or other materials containing confidential information in the bin unless they have been shredded;
- safeguarding and protecting portable electronic devices containing confidential information including but not limited to computers, smartphones, PDAs, CDs, and USB drives;
- disclosing confidential information only to those individuals at RE who have a need to know in order to fulfil their job responsibilities and contract obligations.

Data Security and Data Protection Policy

Action for Peer Reviewer and Employer

Peer Reviewers are responsible for ensuring they work securely and protect both information and resources from loss, damage or unauthorised access. Employer organisations are responsible for ensuring they provide appropriate support to ensure adherence to this policy. If working from home, it is the responsibility of the reviewer and their employer to ensure the working environment and space is suitable for home working.

Data Protection Good Practice

Reviewers must ensure they work in a secure and authorised manner as set out in the key principles below:

- Peer Review activity should not take place in an open plan office environment. An appropriate personal space should be provided to ensure you are able to concentrate on the assessment methodology whilst ensuring confidentiality is observed at all times;
- IT equipment should not be used where it can be overlooked by unauthorised persons;
- Under no circumstances should a Peer Review assessment take place in an open public place, nor should any attempt be made to log onto the SharePoint portal from any open WIFI network or internet café;

- Computers should not be left unattended whilst still logged in. Reviewers must shut down their PC if they leave the room/office, or lock the screen if they are only away from the computer for a short period of time;
- When not in use, files should be stored in lockable filing cabinets or a suitably secure equivalent location;
- If assessments are being undertaken from home, care should be taken to ensure that data is kept secure from unexpected visitors and protected from accidental damage;
- Reviewers are reminded of their obligations regarding the use of personal data including, but not limited to the Data Protection Act 1998, the Data Protection Directive (95/46/EC).