1. TCALM Solutions Ltd ("the company") acts as either data controller or data processor, according to its function. The company is a data processor and acts in accordance with its legitimate interests and legal obligation. At all times the Company acts to ensure the provision of a high-quality service to all users.

2. The company recognizes the necessity of ensuring that appropriate technical and organisational measures are in place that ensure compliance with the relevant current data protection regulations and legislation. These include the measures documented at Appendix 2 of this policy. The confidentiality, integrity and availability of information, in all its forms, are critical to our ongoing functioning and good governance. This policy outlines the Company's approach to information security management and is to be read in conjunction with our Privacy Statement.

3. The core elements to which this policy relates are collection, storage, processing, records, confidentiality, security, incident management, retention and deletion, management, availability, integrity and secure disposal of clients', mediators' and agents' personal and sensitive data.

4. The company is committed to a robust implementation of data protection and information security management. We will do everything possible to ensure the appropriate confidentiality, integrity and availability of data we process or control. The principles outlined in this policy will be applied to all of the physical and electronic information assets for which the Company is responsible. We are specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties in connection with the provision of its services.

5. The company is committed to the provision of a framework for establishing suitable levels of information security for all information systems, (including but not limited to all cloud environments commissioned by or run by the Company, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, damage or abuse of these systems. Continuous improvement of any system will be undertaken in accordance with Assess/Plan/Do/Review principles. The Company undertakes at all times to use software which includes functionality to protect the privacy of individuals, and we will respond to relevant changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

6. The company will ensure that all users are aware of and comply with all current and relevant UK and EU legislation; we document and provide the principles by which a safe and secure information systems working environment can be established for staff and any other authorised users; we ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

7. The company will take all reasonable steps to protect against any potential liability or damage through the misuse of its IT facilities.

8. The company will only collect and process personal and sensitive data that has been obtained fairly and lawfully and for a specific set of purposes connected with business activities or where we have a legitimate purpose under law to do so.

9. The company is responsible for processing all subject access requests in accordance with existing policy and procedure in relation to requests for personal data.

10. The company will take all reasonable steps to ensure that individuals' personal data is kept, used and disposed of in accordance with recognised best practice with regard to data protection. It will maintain data and other confidential information provided by third parties at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security. Classification is documented at Appendix 1 of this policy.

11. The company acknowledges that individuals have the right to expect that appropriate and reasonable safeguards are in operation by the Company and any third party designed to protect the confidentiality, integrity and security of all personal or sensitive data.

12. Staff with responsibility for collecting or collating personal data from third parties must ensure the classification of that information and must handle that information in accordance with its classification level, abiding by any contractual requirements, policies, procedures or systems for meeting those responsibilities. All users must handle information appropriately and in accordance with its classification level.

13. Personal data obtained will be held securely and be available only to those with a legitimate need for access in accordance with its classification level. On this basis, access to information will be on a 'need to know' basis. All personal data will be protected against unauthorised access.

14. The company will not retain personal information for any longer than needed for the purpose for which it was obtained; we will ensure all such data is securely deleted after its use in accordance with this policy or where applicable, at any point if requested to do so by the person who is the subject of the data.

15. Breaches of this policy must be reported in accordance with the company's existing quality assurance system. Any such report will be fully recorded, investigated and resolved expeditiously and in accordance with the company's complaints procedure.

16. Training is provided to all relevant staff to ensure they are aware of their responsibilities under data protection regulations and to clarify what constitutes a personal data breach and how to escalate such a breach.

17. The company will take all reasonable steps to ensure that personal data is securely destroyed.

18. The company follows robust information security procedures recording the following:

(a) the categories of data retained;
(b) how long physical and electronic data is to be stored before being securely destroyed and
(c) which information has been destroyed.

19. The company will keep under review measures taken regarding retention and destruction of data. In particular, the review will ensure the policy and accompanying documents are updated to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

20. This policy was last reviewed on 22 May 2018. Any questions or queries arising from it should be directed to the company at office@tcalmsolutionsltd.co.uk

Appendix 1
Classification Levels
1. Confidential
Definition: Normally accessible only to specified members of staff. Should be held in secure state
Examples: defined Special Categories of personal data such as racial/ethnic origin; political opinion, religion beliefs, trade union

membership, physical/mental health, sexual life, criminal records.

2. Restricted
Definition: Normally accessible only to specified members of staff.
Examples: defined personal data such as information that identifies living individuals including home/work address, age, telephone numbers, schools attended, photographs.

3. Internal Use
Definition: Normally accessible to all staff
Examples: Internal correspondence, final working group papers and notes, committee papers, minutes of directors' meetings.

4. Public
Definition: Accessible to all members of the public
Examples: Annual accounts, published quality reports, promotional or informational literature, redacted minutes of normal committee meetings, information available on the Company website.
Notes:
 Data may move into different classification levels over its lifetime. Where data falls into more than one classification, it will be treated in accordance with the highest applicable category.

Appendix 2
Compliance, Policy Awareness and Disciplinary Procedures
1. Any security breach of the company's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on our information systems. The loss or breach of confidentiality or personal data is an infringement of the GDPR, contravenes the company's data protection policy and may expose the company to criminal or civil liability.

2. The loss or breach of confidentiality of such information may result in the loss of business, financial penalties or legal action. Accordingly, it is essential that all users of the information systems used by the company adhere to the information security procedures and practices outlined in the data protection policy and accompanying documents. All current staff and other authorised users are to be informed of, and are to receive regular and relevant training about, the existence of this policy, together with its appendices and the privacy statement.

3. Any security breach will be handled in accordance with all relevant company policies and appropriate disciplinary policies and procedures.

4. If a member of staff is aware of an information security incident then they must report it to the company at the earliest opportunity.

5. Breaches relating to personal data must be reported immediately to the company.

6. All staff and any third parties authorised to access the company's network or computing facilities or personal data shared with them are required to familiarise themselves with the company's data protection policy, its appendices and the privacy statement