DATA PROTECTION POLICY – GUIDANCE SHEEET

The Data Protection Act covers all personal information, whether held on paper or in electronic format. 'Personal information' is information relating to a living individual who can be identified from that information - may include details such as name, address and date of birth. The Act also defines 'sensitive information', which may include racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, criminal proceedings or convictions. Personal information also includes personal opinions relating to the individual.

What you should do:

- Only hold data about individuals if necessary and for no longer than is necessary
- Endeavour to ensure that data is accurate and up to date, and destroy out of date paper and electronic records properly and confidentially
- Ensure that personal records are held securely — whether on paper (in a locked cabinet) or in an electronic database (password protected).
- Ensure that personal records are accessible only to those who need them
- Seek individuals' written consent to hold their personal data, or establish if consent has already been given
- Report any databases of personal information you hold to the FCA Data Protection Officer
- Do not give personal information to third parties without the individual's written consent.
- Verify the identity of the third party, e.g. via appropriate headed notepaper containing phone numbers that can be checked. Requests by email should not be permitted.
- Respect confidentiality
- Remember that when you put personal information or opinions about an individual in writing, these documents may be accessed and revealed to the individuals they concern
- Let individuals inspect data held about them (while protecting the rights of other data subjects). These are called Subject Access Requests.
- Pass on Subject Access Requests to the Data Protection Officer ASAP
- Ensure that data can be retrieved for inspection at short notice

What you should not do:

- Hold any sensitive personal data, eg, racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexual life, criminal proceedings or convictions.
- Hold personal data without a lawful reason.
- Hold personal data without the individual's consent
- Leave personal data unattended or insecure, eg on a desk, in an unlocked file or computer.
- Give out personal data to third parties without the data subject's written consent
- Give out personal data over the telephone.
- Make public any personal data or photographs of single individuals without the data subject's written consent, eg, on a noticeboard, in publicity material, or on the Web
- Use e-mail for confidential communications
- Destroy or alter data following the receipt of a Subject Access Request.
- Send personal data abroad.