Data Integrity Policy

This document is designed to demonstrate company's compliance with the Data Protection Act 1988 & Data Protection Act & The Privacy & Electronic Communications (EC Directive) regulations 2003.

Appropriate technical and organisational measures are taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data. The data integrity manager, IT department and general management are committed to information security.

Access is controlled to information. The building is card entry only so that only official card holders and their guests can enter the building. Casual passers-by cannot see information. Password protection is used and passwords are only known to official data handlers and are hierarchical, so that data handlers are only aware of passwords relevant to them. Storage media is either destroyed, returned to the supplier or securely cleaned when finished with. Secure printed media is shredded when no longer required. Data is not permitted to leave the premises unless it is to be returned to the supplier or the supplier's nominated handler.

The company premises are protected by intruder and fire alarms linked to the police and fire service respectively, via contract with ADT. All data and important systems are stored on multiple servers and back-up copies are produced regularly and stored off-site or in fire-proof areas. Comprehensive protection is also in place to protect against viruses and other forms of intrusion.

Staff are carefully selected on the basis of their discretion and integrity and their responsibilities made clear. Should an employee be found to be unreliable then their access rights are removed immediately and the staff member subject to disciplinary rules.

If there was a breach of security, our systems keep an audit trail so that a user can be identified in many circumstances. A breach of security would be properly investigated and remedied.

Whether the company is acting as a data controller or a data processor, the Data Protection Act introduces express obligations upon data controllers and data processors. In order to comply with the Seventh Principle the data controller must:

- choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures they take,
- they must take reasonable steps to ensure compliance with those measures,
- ensure that the processing only on instructions from the data controller.
- once processing is complete, ensure all data files are returned to the supplier, destroyed securely or stored securely at the suppliers request.

When dealing specifically with information kept on individuals, The Data Protection Act applies eight principles. The company ensures that all data is;

- Fairly and lawfully processes
- Processed for specific purposes
- Adequate, relevant and not excessive
- Accurate, and where necessary, kept up to date
- Not kept for longer than is necessary
- Processed in line with the rights of the individual
- Kept secure
- Not transferred to countries outside the European Union Economic Area unless there is adequate protection for the information