Information Security Policy Statement

It is the established policy of New Directions to operate within the requirements of a documented Information Security Management Policy as a means to comply with all statutory, regulatory and contractual requirements, and to protect the interests, property and information of the company, and of its clients and employees, against threats or loss.

In pursuance of this policy its stated requirements have been implemented together with the specified requirements of the company's associated Information Security Management Policy.

The purpose of this Information Security Policy Statement is to describe how security is implemented, to give guidance to our employees whose actions can affect the confidentiality and integrity of the business, its product and services, and to illustrate the overall commitment to security issues within our company.

This Information Security Policy Statement, which is not intended as a stand-alone document, is supported by detailed operating procedures and where appropriate, by quality management systems, to form a set of working documents, which define our company's security activities.

The Information Security Management Policy is subject to regular review, in order to provide effective assurance that all aspects of company, employee and customer specified security requirements are being implemented.

It is company policy to ensure that the use of documents, computers, mobile computing, mobile communications, mail, voicemail, voice communications in general, multimedia, postal services and fax machines must be controlled to prevent unauthorised use and to reduce security risks.

All employees have a responsibility not to compromise the company, e.g. by sending defamatory or harassing electronic mail, or by making unauthorised purchases, and must also be aware that the confidentiality and integrity of information transmitted by email or facsimile may not be guaranteed.

Access by employees to the Internet is restricted to business use only (unless otherwise authorised by a manager) and any breach of this policy may result in disciplinary action being taken.

The Service Manager is responsible for managing information security, and they will also ensure that all employees are trained to understand, implement and maintain the security objectives set out in this policy statement and as detailed in the company's Information Security Management Policy.

We publish this policy statement in the knowledge that the security of our company and its employees, products and client services, and our ongoing good security reputation, depend upon the everyday security awareness and actions of all our employees, both onsite and offsite.

I am wholly committed to the Information Security Management Policy, and hereby state that it is the responsibility of every individual employee of the company to ensure that all security plans, standards, procedures, work instructions and actions fully meet with agreed company and customer requirements.

Signature: .....

Job title: .....

Mark Fox

Managing Director