Information Security

Policy Document

1. Introduction

1.1 Lakethorne recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, the company will facilitate the secure and uninterrupted flow of information, both within the company and in external communications.

2. Definition

2.1 For the purposes of this document, information security is defined as the preservation of:

- Confidentiality - protecting information from unauthorised access and disclosure;
- Integrity - safeguarding the accuracy and completeness of information and processing methods; and
- Availability - ensuring that information and associated services are available to authorised users when required.

2.2 Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

3. Protection of Personal Data

The company is committed to being transparent about how it collects and uses the personal data of its workforce, customers and suppliers, and to meeting its data protection obligations in accordance with the requirements of the GDPR. The company's separate Data Protection Policy sets out the company's commitment to data protection, and individual rights and obligations in relation to personal data.

4. Information Security Responsibilities

4.1 The company believes that information security is the responsibility of all members of staff. Every person handling information or using company information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the company.

4.2 This policy is the responsibility of the Director and supervision of the policy will be undertaken by the Senior Management Team. This policy may be supplemented by more detailed interpretation for specific sites, systems and services. Implementation of this Information Security Policy is managed through the Administration Manager who has responsibility for IT at the company.

5. Information Security Education and Training

The company recognises the need for all staff to be aware of information security threats and concerns, and to be equipped to support the company Information Security Policy in the course of their normal work. The Administration Manager shall implement a training programme for each class of users and shall provide information and further training in information security matters to answer particular requirements.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under the Data Protection policy, will receive additional training to help them understand their duties and how to comply with them.

6. Compliance with Legal and Contractual Requirements

6.1 **Authorised Use** - Company IT facilities must only be used for authorised purposes as outlined in the Staff Handbook. The company may from time to time monitor or

investigate usage of IT facilities and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings.

Monitoring is in the company's legitimate interests and is to ensure that the company's policy on email and internet use is being complied with.

Information obtained through monitoring will not be disclosed to third parties, unless the Company is under a duty to report matters to a regulatory authority or to a law enforcement agency.

6.2 **Access to Company Records** - In general, the privacy of users' files will be respected but the company reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with company policies and regulations, and to determine which records are essential for the company to function administratively. Except in emergency circumstances, authorisation for access must be obtained from the Director and shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

6.3 **Protection of Software** - To ensure that all software and licensed products used within the company comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts, the company will carry out checks from time to time to ensure that only authorised products are being used, and will keep a record of the results of those audits. Unauthorised copying of software or use of unauthorised products by staff may be grounds for disciplinary, and where appropriate, legal proceedings.

7. Retention, Storage and Disposal of Information

7.1 The company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

7.2 Where the Company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

7.3 Personal data is only retained for as long as there is a clear business need for it and is securely destroyed after that period is passed.

8. Reporting

8.1 All staff should immediately inform the Director if they observe or suspect security incidents where a breach of the company's security policies has occurred, any security weaknesses in, or threats to, systems or services.

8.2. Software malfunctions should be reported to the Commercial Manager.

8.3 Employees have a duty to report data breaches immediately. Serious data breaches will be reported to the Information Commissioner's Office.

9. Business Continuity

The company will implement, and regularly update, a business continuity management process to counteract interruptions to normal company activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

Signed: ..... Date: January 2019

Richard Bent

Managing Director Next review date: January 2020