R B Tree and Landscape Limited

Data Protection Policy

1. Introduction

R B Tree and Landscape Limited 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. We shall take guidance from and shall comply with the Data Protection Act 1998 and the General Data Protection Regulations 2018.

We believe that security is an integral part of the information sharing which is essential to corporate endeavour and the policies outlined below are intended to support information security measures throughout the organisation.

2. Definition

For the purposes of this document, information security shall be defined as:

- The preservation of confidentiality
- Protecting information from unauthorised access and disclosure
- Safeguarding the accuracy and completeness of information and processing methods
- Ensuring that information and associated services are available to authorised users when required

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 organisation holds and processes information about employees, customers and enquirers for commercial purposes.

When handling such information, we shall comply with the General Data Protection Regulations 2018.

All staff shall be briefed on the collection, storage, use and handling of their personal data during their induction training. The Employee Privacy Notice shall be displayed on the company noticeboard.

All enquirers and customers shall be provided with a Customer Privacy Notice along with business terms and conditions which explain how their date will be collected, stored, used and handled.

4. Information Security Responsibilities

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

This Policy and the supervision of this policy shall be the responsibility of the Director.

This policy may be supplemented by more detailed interpretation for specific sites, systems and services.

5. Information Security Education and Training

The organisation recognises the need for all staff to be aware of information security threats and concerns, and to be equipped to support the organisations security policy during their normal work.

All members of staff shall be briefed on our data protection procedures as they apply to their job roles.

6. Compliance with Legal and Contractual Requirements

The Company's IT facilities must only be used for authorised purposes.

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.

The Company shall only permit the inspection and monitoring of operational logs by computer operations personnel and system administrators. Disclosure of information from such logs, to officers of the law or to support disciplinary proceedings, shall only occur:

- When required by and consistent with law
- When there is reason to believe that a violation of law or of a Company policy has taken place
- When there are compelling circumstances where failure to act may result in:

    - Significant bodily harm
    - Significant property loss or damage
    - Loss of significant evidence of one or more violations of the law
    - Significant liability to the Company or to members of the Company community

The privacy of users' files shall be respected but the Company reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with organisational policies and regulations, and to determine which records are essential for the organisation to function administratively or to meet its commercial obligations.

Except in emergency circumstances, authorisation for access must be obtained from the Directors or their nominee, and shall be limited to the least perusal of contents and the least action necessary to resolve the situation

To ensure that all software and licensed products used within the organisation comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts the organisation shall carry out checks from time to time to ensure that only authorised products are being used, and shall 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.

The organisation shall maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of computers, including laptops, shall comply with best practice to ensure that up-to-date virus protection is maintained on their machines.

7. Retention and Disposal of Information

All staff shall have a responsibility to consider security when disposing of information in the course of their work.

8. Reporting

All staff should report immediately to the Director, any observed or suspected security incidents where a breach of the organisations security policies has occurred, any security weaknesses in, or threats to, systems or services.

Software malfunctions should be reported to the Director.

9. Business Continuity

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