Information Security, Confidentiality & Access Policy

1. PURPOSE

The purpose of this policy is to ensure that Pipe & Piper Limited:-

(a) fully complies with its legal obligations in relation to data security and confidentiality under the GDPR and the Data Protection Act 2018;

(b) provides its clients with a service that is fully compliant with such Data Protection laws and ensures that our clients are fully compliant with their obligations under Article 24 of the GDPR to use "appropriate technical and organisational measures" to ensure processing complies with the GDPR.

(c) Takes all appropriate and reasonable steps to protect both its own business and that of its customers from data loss, theft, corruption, unauthorised access or misuse.

Data security best practices develop over time as the underlying technologies and related security threats evolve, so we will keep this policy and the detailed measures necessary to implement it under continual and routine review.

This policy uses various definitions:

Data Protection Legislation: means the UK Data Protection Legislation and any other European Union legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

UK Data Protection Legislation: means all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679); EU Regulation 2018/151; the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended, the Network and Information Systems Regulations 2018 (SI 2018/506)

The terms **Personal Data**, **Personal Data Breach**, **Controller** and **Processor** shall have the meanings ascribed to them by the Data Protection Legislation.

User Personal Data means personal data relating to the users of cloud based Apps, websites, software and content management systems (**Users**) which Pipe & Piper maintains for its clients.

Client Personal Data means personal data relating to our clients and potential clients who visit our website at https://pipeandpiper.co.uk **Our Website**.

2. DATA SECURITY

We will use appropriate technical and organisational measures to ensure a level of security for the Personal Data we process that is appropriate to the obligations imposed on us by the Data Protection Legislation (which, due to our size, do not include the Network and Information Systems Regulations 2018 (SI 2018/506)), our size, scope and nature of our business, our available resources, the amount of Personal Data that we maintain on behalf of others and identified risks.

Those measures shall protect the confidentiality, integrity and availability of Personal Data and protect against unauthorised or unlawful processing, accidental loss or destruction or damage, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected and having regard to the state of technological development and the cost of implementing any measures.

Those measures shall involve the use if best available technology not entailing excessive cost and specifically shall include:-

(i) **Confidentiality** – this is secured by only allowing people who have a need to know and are authorised to use Personal Data can access it;

(ii) **Integrity** – For Client Personal Data this is secured by ensuring that such Personal Data is accurate and suitable for the purpose for which it is processed. We are not responsible for maintaining or monitoring the integrity of User Personal Data; and

(iii) **Availability of Personal Data** – This is secured by the security of our IT systems and that regular back-ups of information we hold are made so that our clients and Users are able to access Personal Data when they need it for authorised purposes and that access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by Pipe & Piper.

(iv) **Asset Management** - All assets (software and electronic information processing equipment and service utilities) will be documented and accounted for.

(v) **Physical and Environmental Security** - the housing of information processing facilities in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls are in place to deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack.

(vi) **Access Control** - Access to all information will be controlled and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed, and will include consideration of multiple factors as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

(vii) **The use of firewalls** – both software and hardware firewalls are used and updated in accordance with industry standards to prevent external cyber threats associated with cloud technologies.

(viii) **Passwords** - The use of passwords to access laptops and servers and ensuring that such passwords are changed at least every 60 days. Access to all servers we use to hold personal data is password protected so that where the servers are owned or physically located with third parties, those third parties cannot access any information on such servers. Any such passwords are changed regularly.

Passwords are chosen to make them very secure. Access to such passwords is not given to any businesses which own or operate such servers, which should make it impossible for them to access any information including personal data held on such servers.

(ix) **Anti-virus software** - the regular use of updated anti-virus software, supplied and updated by trusted industry leaders.

(x) **Additional** - Servers are UK based. Redundancy servers are also UK based (off site). SSL 256 bit encryption – Connections are encrypted and authenticated using:

- TLS 1.2 protocol, ECDHE_RSA
- P-256 key exchange
- AES_128_GCM cipher
- The signature algorithm uses a SHA256RSA
- The dedicated server uses the latest stable version of Plesk (v17.8.11) which includes several security features and modules in addition to:
- Fail2Ban
- KernelCare Extension
- Hosted websites from our sever benefit from using http2 which speeds up loading time and is more secure because it makes TLS connections mandatory
- 99.9% uptime guarantee with redundancy

We regularly evaluate and test the effectiveness of such measures to ensure security of our Processing of Personal Data.

All our employees are required to follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

We only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

3. BUSINESS CONTINUITY MANAGEMENT AND BACKING UP OF PERSONAL DATA

Pipe & Piper shall develop a back-up schedule, perform scheduled back-ups, provide routine and emergency data recovery, and manage the archiving process for its clients, in accordance with levels of service agreed with our clients on a case by case basis.

The back-up schedule shall include at least weekly full back-ups and daily incremental back-ups. In the event of data loss, Pipe & Piper shall provide recovery services to try to restore the most recent back-up.

4. DATA ACCESS

Employees of Pipe & Piper will never access, inspect, use, alter or modify **User Personal Data** unless:-

(a) Such processing has been agreed in advance with the relevant client in writing and is even then only undertaken to the minimum extent strictly necessary to achieve the purpose behind such access and any copies of any personal data

obtained by us as a result shall be kept confidential, not used for any other than the client's stated purpose, processed fully in accordance with the Data Protection Legislation and shall be destroyed as soon as such purpose has been achieved.

(b) Such processing is strictly necessary to enable us to comply with our obligations at law or pursuant to any contract with our clients. Where such access is required then we will notify our clients accordingly and any such access will be kept to a strict minimum, with any personal data thereby extracted retained for the absolute minimum length of time required and processed in a manner fully compliant with the Data Protection Legislation.

4. DATA CONFIDENTIALITY

All our employees and third party contractors with whom we share confidential information are bound by written obligations of confidentiality, limiting their ability to lawfully disclose or use such information for any purpose other than the purpose for which it was disclosed.

5. DATA BREACHES

The GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator within 72 hours of becoming aware of the breach and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects, our clients and any applicable regulator where we are legally required to do so.