LINSTONE CHINE MANAGEMENT COMPANY LTD

DATA RETENTION & DISPOSAL POLICY

Affects:		All Staff, Members & Directors of the Company	
Attachments:		None	
Rev.	Date	Authorising Signature	Title
0	6th April 2019		Chairman

Definitions

For the purpose of this document Linstone Chine consists of the following 2 companies. Linstone Chine Management Company and Linstone Chine Holiday Services.

Introduction

This Policy sets out the obligations of Linstone Chine regarding the retention of personal data collected, held, and processed by the Company in accordance General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person. Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- The personal data is no longer required for the purpose for which it was originally collected or processed
- When the data subject withdraws their consent;
- The individual objects to the processing of their personal data and the Company has no overriding legitimate interest;
- When the personal data is processed unlawfully (i.e. in breach of the GDPR);
- When the personal data has to be erased to comply with a legal obligation; or
- Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company), the period for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

Aims and Objectives

The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits are complied with.

Scope

This Policy applies to all personal data held by the Company and by any third-party data processors processing personal data on the Company's behalf.

Personal data, as held by the Company is stored in the following ways and in the following locations:

- Company computers and mobile devices used for company business located at

Linstone Chine's Office at Monks Lane

- Computers and mobile devices owned by employees, agents, and sub-contractors
- Physical records stored at Linstone Chine's Office at Monks Lane

Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set within the Privacy Policy.

Technical and Organisational Data Security Measures

The following technical measures are in place within the Company to protect the security of personal data.

Personal data may only be transmitted over secure networks;

Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using a reputable delivery service;

No personal data may be shared informally and if access is required to any personal data, such access should be formally requested via a company Director;

Hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;

Personal data must be handled with care at all times and should not be left unattended or on view;

Computers used to view personal data must always be locked before being left unattended;

No personal data should be stored on any mobile device whether such device belongs to the Company or otherwise without the formal written approval of the individual and then strictly in accordance with all instructions and limitations described at the time the approval and for no longer than is necessary;

No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection and Disposal Policy and the Privacy Policy.

All personal data stored electronically should be backed up and the backups stored securely.

All electronic copies of personal data should be stored securely using passwords and encryption;

All passwords used to protect personal data should be changed regularly and must be secure;

Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method.

All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

No software may be installed on any Company-owned computer or device without prior approval;

Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the client manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;

Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;

All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;

All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Data Disposal

Upon the expiry of the data retention period of 7 years as set out below in this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- Personal data stored electronically (including any and all backups thereof) shall be deleted
- Special category personal data stored electronically (including any and all backups thereof) shall be deleted
- Personal data stored in hardcopy form shall be shredded.

Data Retention

As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

Different types of personal data may be retained for different periods, as set out below.

When establishing and/or reviewing retention periods, the following shall be taken

into account:

- The objectives and requirements of the Company;
- The type of personal data in question;
- The purpose(s) for which the data in question is collected, held, and processed;
- The Company's legal basis for collecting, holding, and processing that data;
- The category or categories of data subject to whom the data relates;

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Roles and Responsibilities

The Company's Data Protection Officer is **Nick Kenworthy**

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

The Data Protection Officer or The Company Directors shall be directly responsible for ensuring compliance with the above data retention for all data within their departments.

Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

This Policy has been approved and authorised by:

Name:	Nigel Eastement
Position:	Chairman
Date:	6/4/2020
Due for Review by:	6/4/2020
Signature: