DATA RETENTION POLICY

Version 0.0

25th April 2018

VERSION HISTORY

Version	Author	Revision Date	Approved By	Approval Date	Comments
0.0	Stephen Grant	25/04/2018			Initial Draft

Table of Contents

1. Introduction

This policy sets out how Mouse Click Systems Ltd. will approach data retention and establishes processes to ensure we do not hold data for longer than is necessary.

This Policy applies to all business units, processes, and systems in all the countries in which Mouse Click Systems Ltd. conducts business and has dealings or other business relationships with third parties.

This Policy applies to all Company officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and/or sensitive personal data). It is the responsibility of all of the above to familiarise themselves with this Policy and ensure adequate compliance with it.

This policy applies to all information used at the Company. Examples of documents include:

- Emails
- Hard copy documents
- Soft copy documents
- Video and audio
- Data generated by physical access control systems

1.1 Roles and Responsibilities

Mouse Click Systems Ltd. is the Data Controller and will determine what data is collected, retained and how it is used. The Data Protection Officer for Mouse Click Systems Ltd. is **Stephen Grant**. They, together with the band's trustees and committee, are responsible for the secure, fair and transparent collection and use of data by Mouse Click Systems Ltd. Any questions relating to the collection or use of data should be directed to the Data Protection Officer.

2. Retention Rules

2.1 Retention General Principle

In the event, for any category of documents not specifically defined elsewhere in this Policy (and in particular within the Data Retention Schedule) and unless otherwise mandated differently by applicable law, the required retention period for such document will be deemed to be 3 years from the date of creation of the document.

2.2 Retention General Schedule

The Data Protection Officer defines the time period for which the documents and electronic records should to be retained through the Data Retention Schedule.

As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from Member States authorities, if there is a chance records of personal data are needed by the Company to prove compliance with any legal requirements; or
- When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law.

2.3 Safeguarding of Data during Retention Period

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The responsibility for the storage falls to the Data Protection Officer.

2.4 Destruction of Data

The Company and its employees should therefore, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See Appendix for the retention schedule. Overall responsibility for the destruction of data falls to the Data Protection Officer.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data

Protection Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the Company's Personal Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevents the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the company's IT Security Policy.

The Data Protection Officer shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

2.5 Breach, Enforcement and Compliance

The person appointed with responsibility for Data Protection, the Data Protection Officer has the responsibility to ensure that each of the Company's offices complies with this Policy. It is also the responsibility of the Data Protection Officer to assist any local office with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to Data Protection Officer. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to the Company's reputation, personal injury, harm or loss. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Company premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

3. Document Disposal

3.1 Routine Disposal Schedule

Records which may be routinely destroyed unless subject to an on-going legal or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies;
- Requests for ordinary information such as travel directions;
- Reservations for internal meetings without charges/external costs;
- Transmission documents such as letters, fax cover sheets, e-mail messages, compliments slips and similar items that accompany documents but do not add any value;
- Message slips;
- Superseded address list, distribution lists etc.;
- Duplicate documents such unaltered drafts, snapshot printouts or extracts from databases and day files;
- Stock in-house publications which are obsolete or superseded; and
- Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organizations.

In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.

3.2 Destruction Method

Level I documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

Level II documents are proprietary documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be cross-cut shredded and then placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

Level III documents are those that do not contain any confidential information or personal data and are published Company documents. These should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

4. Changes to this Data Retention Policy

We reserve the right to make changes to this Data Retention Policy at any time. Any changes will be posted in this Data Retention Policy and material changes will be prominently notified on the respective website or application this Data Retention Policy applies to or will be otherwise communicated to you prior to the change becoming effective. We encourage you to regularly review this Data Retention Policy to make sure you are aware of any changes and how your information may be stored.

4.1 Updates

This Data Retention Policy was last updated on **25th April 2018**

5. Contacting Us

If you any questions or comments about this Data Retention Policy, please contact us:

Mouse Click Systems Ltd
Brunel House
340 Firecrest Court
Centre Park
Warrington
Cheshire
WA1 1RG

Email: dataprotection@mouseclicksystems.co.uk

Website: http://www.mouseclicksystems.co.uk/contact-us

You can contact the Information Commissioners Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113

Website: https://ico.org.uk/global/contact-us/email/

Appendix A: Retention Periods

Category	Retention Period
Company Documents	
Accounting Records and Supporting Documents	7 Years
Formal Company Documents • Statutory Books • Board Meetings • Resolutions	Indefinitely
Meeting Minutes	10 Years
Personnel Files	
Payroll and Wage Records	7 Years
PAYE Records	7 Years
Job Applications and Interview Records	6 Months
Personnel and Training Records	7 Years after end of employment
Bank Records	No more than 1 Month after end of employment
Business Records	
VAT Records (electronic or paper formats)	7 Years
Corporation Tax Records	7 Years
Contracts	
Contracts	Indefinitely
Tender Documents	Indefinitely
Operation and Monitoring	Indefinitely
Customer Records	
CRM Data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries	Retained whilst organisation remains a customer or deleted by user. Once an organisation requests all records to be deleted, data will be removed from the back-ups within 3 months
Non-Customer Records	
Name, email address	Kept until person unsubscribes / requests to be removed from system