LimeCulture
Data Retention, Management and Deletion Policy

Statement

1. LimeCulture's nominated lead for data protection is the Director of Operations.

2. LimeCulture is committed to keeping accurate and relevant records of the organisation's training and development, consultancy, research, programme, and back-office activities. For the avoidance of doubt all records created by the LimeCulture core team in the course of their work are covered.

Audit

3. To ensure that the organisation is adhering to the Knowledge Management Policies and data protection legislation, a programme of audit will be implemented by the nominated lead for data protection, and reports made to the Senior Leadership Team (SLT) on a regular basis.

4. The audit will include:

   a. Review of appropriateness of access to team folders

   b. Review of individual patterns of access to files, folders, and documents

   c. Review of use of email, including volumes of information

   d. Review of use of two-step verification, strength of passwords and a requirement to change passwords regularly

   e. Review of requests made by individuals for access to personal data, correction of, or deletion of records

   f. Any risks, incidents, or potential personal data breaches identified through audit activity will be escalated in line with LimeCulture's data protection and incident management procedures.

Data Retention

5. Information is an asset, and must be managed appropriately to support organisational needs, legal obligations, and data protection requirements.

6. As a part of this policy all core team members are required to document actions and decisions by keeping accurate records, and they should also follow the guidance in relation to the maintenance

and disposal of those records. This is because our organisational records have a value associated with our business needs and obligations, or the records may be information assets, in line with this policy and relevant legal and regulatory requirements.

7. Factors that need to be considered when determining the value of a record are:

   a. Whether the record contains personal data

   b. The function that the records support

   c. The risks to the business of not being able to access the information

   d. The importance of the records for protecting the interests and the legal rights of the organisation

   e. Archival value (corporate memory, historical, cultural purposes)

   f. Management and operational requirements

   Least Privilege

8. Access to the LimeCulture DropBox system where we hold personal data is authorised by the nominated lead for data protection. User permissions will be regularly reviewed, and user permissions restricted to the absolute minimum (known as 'least privilege'). Each user will continue to be assigned their own username and password to ensure accountability, and must enrol on two- step verification. Access rights will be reviewed regularly and revoked promptly where no longer required,

   Provision of Access to DropBox for External Users

9. In order to facilitate delegates downloading course materials, or uploading evidence for accreditation, it will sometime be useful to facilitate access to DropBox for external people.

10. This access must be limited in time and scope and a record of this access must be maintained by the core team member. Wherever possible alternative methods of facilitating access to materials should be used. This could include making materials downloadable from the website. Access should only be granted where necessary and must be removed as soon as it is no longer required.

    File naming convention

11. To support core team members locate files, and to support version control in cases where more than one person may be working on a document, or where draft documents are produced before a final version is agreed this naming convention should apply to folders and files.

12. To maintain compliance with the requirements of UK GDPR and data protection legislation where a file contains personal data the file name should contain a date and clearly indicate the presence of personal data (e.g.‘PD’).

Table 1: File Naming Convention

1	Use capital letters to delimit words, not spaces. Use capital letters for acronyms.	This reduces the length of file names, but using capital letters means you can still read it.	Isva Risk Management ISVARiskManagement
2	Keep file names short but meaningful. If the file contains personal data, it should include 'PD' at the end of the file name.	Long paths and URLs increase errors and are more difficult to recognize. Some words add length but not meaning, like 'the' or 'of'.	Approaches to the management of risk for ISVAs ISVA Risk Management Conference AttendeesPD
3	If using a date add it back to front: YYMMDD. Files containing data must always have a date in the file name.	This maintains chronological order of records in DropBox	1Feb2018Agenda 180201 Agenda LimeCulture Employee List 180922LimeCulutreEmployeesListPD
4	If including a version number in the file name always give it as a two-digit number, not a single digit at the end of the file name.	Not including a 0 for numbers 1 to 9 will mean ordering errors in the file list	FilingProceduresV1 FilingProceduresV01
5	When a final version is agreed this should be labelled 'FINAL'.	Keeping all the file names the same except for the version control means the most recent can be easily identified	2018 Conference Agenda ISVA V1 2018 Agenda Conference V2 ISVA 2018ISVAConferenceAgendaV1 2018ISVAConferenceAgendaFINAL
6	Avoid common words at the start of file names	Using words like 'draft' or 'agenda' is unlikely to help you find the document	draft Agenda Team Meeting MeetingAgendaDraft
7	Use Meaningful folder names	Names should indicate folder contents	Office/Jo/MISC Office/Operations/Timetables

Record Deletion

13. As a business it is important to be clear what types of records are held and how long they should be kept. Records should be regularly reviewed to ensure they are retained only for as long as necessary and are securely deleted or disposed of when no longer required, in line with this policy and data protection legislation.

14. This policy is reviewed regularly to ensure it remains aligned with current legislation, guidance, and organizational practice.

15. Making Decisions about Retention or Disposal of Records:

