LORD'S TAVERNERS
Empowering young people through cricket

Lord's Taverners Data retention policy (GDPR and DPA 2018) (UK)

Contents:-

1. About this policy

2. Scope of the policy

3. Guiding principles

4. Roles and Responsibilities

5. Types of Data and Data classifications

6. Retention periods

7. Storage, Backup and disposal of Data

8. Special Circumstances

9. Where to go for advice and questions

10. Breech reporting and Audit

11. Other relevant policies

Annex A. Definitions
Annex B. Retention Schedule

Update record:

Date Approved:	25th Jan 23 -GFC
Date of Next review:	Jan 2025
Related Policies:	

1. ABOUT THIS POLICY

1.1 The corporate information, records, and data of LORD'S TAVERNERS is important to how we conduct business and manage employees.

1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

1.3 This Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.4 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. SCOPE OF POLICY

2.1 This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

2.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices in accordance with our Bring Your Own Device Policy

2.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

3. GUIDING PRINCIPLES

3.1 Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We regularly monitor and audit compliance with this policy and update this policy when required.

4. ROLES AND RESPONSIBILITIES

4.1 Responsibility **of all employees**. We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All employees must comply with this policy, the Record Retention Schedule, any communications suspending data disposal and any specific instructions from the Data Protection Officer (DPO). Failure to do so may subject us, our employees, and contractors to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

4.2 The DPO is responsible for identifying the data that we must or should retain, and determining, in collaboration with other departments, the proper period of retention. It also arranges for the proper storage and retrieval of data, co-ordinating with outside vendors where appropriate. Additionally, the DPO handles the destruction of records whose retention period has expired.

4.3 We have a designated Organisational Improvement and Compliance Manager. Who has oversight of all departments to ensure all data is handled, processed, and stored correctly. Along with ;

- Administering the data management programme;
- Helping department heads implement the data management programme and related best practices;
- Planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and
- Providing guidance, training, monitoring and updating in relation to this policy.

4.4 Data Protection Officer. Our Data Protection Officer (DPO) is responsible for advising on and monitoring our compliance with data protection laws which regulate personal data. Our DPO works with our Records Management Department on the retention requirements for personal data and on monitoring compliance with this policy in relation to personal data.

5. TYPES OF DATA AND DATA CLASSIFICATIONS

5.1 Formal **or official records.** Certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see *Paragraph 6.1* below for more information on retention periods for this type of data.

5.2 Disposable **information**. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of LORD'S TANERNERS and retained primarily for reference purposes.
- Spam and junk mail.

Please see *Paragraph 6.2* below for more information on how to determine retention periods for this type of data.

5.3 Personal **data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). See *Paragraph 6.3* below for more information on this.

5.4 Confidential **information belonging to others**. Any confidential information that an employee may have obtained from a source outside of [ORGANISATION NAME], such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

5.5 Data **classifications.** Some of our data is more confidential than other data.

6. RETENTION PERIODS

6.1 Formal **or official records.** Any data that is part of any of the categories listed in the Record Retention Schedule contained in the Annex to this policy, must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Records Management Officer.

6.2 Disposable **information.** The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

6.3 Personal **data.** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data.

6.4 What **to do if data is not listed in the Record Retention Schedule.** If data is not listed in the Record Retention Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Record Retention Schedule, or if you are unsure, please contact the Records Management Department**.**

7. STORAGE, BACK-UP AND DISPOSAL OF DATA

7.1 Storage**.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

7.2 Destruction. Our Organisational Improvement and Compliance Manager is responsible for the continuing process of ensuring data owners are identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be co-ordinated with the DPO.

7.3 The destruction of data must stop immediately upon notification from the DPO that preservation of

documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). Destruction may begin again once the DPO lifts the requirement for preservation.

8. SPECIAL CIRCUMSTANCES

8.1 Preservation **of documents for contemplated litigation and other special situations.** We require all employees to comply fully with our Record Retention Schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the DPO informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the DPO determines those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

8.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the DPO and Organisational Improvement and Compliance Manager at data@lordstaverners.org.

8.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

9. WHERE TO GO FOR ADVICE AND QUESTIONS

9.1 Questions **about the policy.** Any questions about retention periods relevant to you should be raised with the DPO. Any questions about this policy should be referred to Organisational Improvement and Compliance Officer data@lordstaverners.org , who is in charge of administering, enforcing, and updating this policy.

10. BREACH REPORTING AND AUDIT

10.1 Reporting **policy breaches.** We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depend largely on employees. If you feel that you or someone else may have breached this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with the Records Management Officer at the next level above your direct supervisor. If employees do not report

inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

10.2 No one will be subject to and we do not allow, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

10.3 Audits. Our DPO and the Organisational Improvement and Compliance Manager will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice to ensure we are in compliance with relevant new or amended laws, regulations or guidance.) Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

ANNEX A

DEFINITIONS

Data: all data that we hold or have control over and therefore to which this policy applies. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

Data Protection Officer: our Data Protection Officer who is responsible for advising on and monitoring compliance with data protection laws.

Data Retention Policy: this policy, which explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

Disposable information: disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule.

Formal or official record: certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

Non-personal data: data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised.

Personal data: any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data such as health data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Records Management Department: the department responsible for identifying the data that we must or should retain, and determining, in collaboration with the [Legal Department **OR** [OTHER

DEPARTMENT]], the proper period of retention. It also arranges for the proper storage and retrieval of data, co-ordinating with outside vendors where appropriate and handles the destruction of [some] records whose retention period has expired.

Records Management Officer: the Records Management Officer is head of the Records Management Department and is responsible for administering the data management programme, helping department heads implement it and related best practices, planning, developing, and prescribing data disposal policies, systems, standards, and procedures and providing guidance, training, monitoring and updating in relation to this policy.

Record Retention Schedule: the schedule attached to this policy which sets out retention periods for our formal or official records.

Storage limitation principle: data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed. This is referred to in the GDPR as the principle of storage limitation.

ANNEX B

RECORD RETENTION SCHEDULE

LORD'S TANERNERS establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

Employees should comply with the retention periods listed in the record retention schedule below, in accordance with LORD'S TANERNERS Data Retention Policy.

If you hold data not listed below, please refer to LORD'S TANERNERS Data Retention Policy. If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this record retention schedule, please contact Organisational Improvement and Compliance Manager data@lordstaverners.org

Category	Examples and Retention period
Financial records	Purchase ledger, sales ledger, cash book payments etc. Payroll data **Current year plus six**
Complaints	Correspondence with complainants **Current year plus 6**
Contractual arrangements	Service level agreements Legal contracts Tender documentation **Life of contract plus 6 years**
Personnel records	Wide variety of specific retention limits – please see separate Personnel Data **Retention Schedule from six months to 75 years**
Health and Safety records	**Retention Schedule Up to 80 years**

Safeguarding records	Records in regards Safeguarding **Retention current year plus 5 unless litigation**

Document description - Employment and career	Retention period - Years	Action following retention
Written particulars of employment Contracts of employment, including the Certificate of Qualification or its equivalent and including terms and conditions(LMS)	Retain for current staff. Former staff Termination + 2	Securely deleted and destroyed
Membership	Retain for life of membership + 6 years	Securely deleted and destroyed
Job History - consolidated record of whole career and location details (paper or electronic)	Retain for current staff. Former staff Termination + 2	Securely deleted and destroyed
Name, Current address details, telephone number/mobile number/ personal email address	Retain and update annually	Securely deleted and destroyed
Curriculum Vitae and covering letters	Retain for current staff. Former staff Termination + 1	Securely deleted and destroyed
Current staff details	Retain and update annually	Securely deleted and destroyed
Former staff details	Date of termination + 6	Securely deleted and destroyed
Staff career development reviews (Appraisals)	Retain for current staff. Former staff Termination + 2	Securely deleted and destroyed
Occupational health report	Date of termination + 4	Securely deleted and destroyed
Exit interview forms	Date of termination + 2	Securely deleted and destroyed
Employee tribunal records	Date of termination + 1	Securely deleted and destroyed
Parental leave requests	Date of termination + 1	Securely deleted and destroyed
	Date of termination + 1	Securely deleted and destroyed

Pension documentation(Aviva)	Date of termination + 6	Securely deleted and destroyed
References	Retain for current staff Former staff + 1	Securely deleted and destroyed
Holiday/leave records	Date of termination + 1	Securely deleted and destroyed
Disclosure certificates(DBS)	Record receipt only, 3 years of receipt	Securely deleted and destroyed
Disciplinary records	12 month from disciplinaryUnless litigation	Securely deleted and destroyed
Grievance records	12 month from Grievance Unless litigation pending	Securely deleted and destroyed
Unsuccessful post applications	One month	Securely deleted and destroyed
Recruitment documents	One Month	Securely deleted and destroyed
Interview notes(Matrix)	One month	Securely deleted and destroyed
Bank account details	Current tax year + 5	Securely deleted and destroyed
Promotion, temporary promotion and/or substitution documentation (offer letter)	Retain for current staff. Former staff Termination + 2	Securely deleted and destroyed
Qualifications	Date of termination + 2	Securely deleted and destroyed
Travel and subsistence - claims and authorisation	Current year + 5	Securely deleted and destroyed

Document description – Pay and Pension	Retention period - Years	Action following retention
Bank details	Current tax year + 5	Securely deleted and destroyed
Salary details	Current tax year + 5	Securely deleted and destroyed
P45	Current tax year + 5	Securely deleted and destroyed

P60	Current tax year + 2	Securely deleted and destroyed
Statutory maternity pays documents	Current tax year + 5	Securely deleted and destroyed
Other maternity pay documentation	Current tax year + 5	Securely deleted and destroyed
Personal payroll history, including record of pay, performance pay, overtime pay, allowances, pay enhancements, other taxable allowances, payment for untaken leave, reduced pay, no pay, maternity leave	Current tax year + 5	Securely deleted and destroyed
Pensions estimates and awards	Outsourced agree with pension provider-Legal requirement	Securely deleted and destroyed
Record of: • Full name and date of birth • National Insurance number • Pensionable pay at leaving • Reason for leaving and new employer's name (where known) • Amount and destination of any transfer value paid • Amount of any refund of contributions • Amount and date of any Contributions Equivalent Premium paid • Medical/Disability declaration	Retain for current staff. Former staff Termination + 5	Securely deleted and destroyed
Resignation, termination and/or retirement letters	Retain for current staff. Former staff Termination + 2	Securely deleted and destroyed
Complete sick absence record showing dates and causes of sick leave	Retain for current staff. Former staff Termination + 2	Securely deleted and destroyed
Papers relating to disciplinary action which has resulted in any changes to terms and conditions of service, salary, performance pay or allowances	Closure of incident +12 months. Unless under litigation	Securely deleted

		and destroyed
Authorisation for deputising, substitution allowance and/or overtime/travel time claim	Retain for current staff. Former staff Termination + current tax year + 5	Securely deleted and destroyed
Advances for: • Train season tickets • Car Allowance • Season tickets loan	Retain for current staff. Former staff Termination + current tax year + 5	Securely deleted and destroyed

Document description - Finance	Retention period - Years	Action following retention
Annual company accounts	Previous Year + 2 + Archive	Archived
Monthly financial statements	Current year + 2	Archieved,Securely deleted and destroyed
External audit reports	Previous Year + 2 + Archive	Archived
Tax documentation	Current year + 5	Securely deleted and destroyed
VAT administration	Current year + 5	Securely deleted and destroyed
Travel/Staff expenses	Current year + 5	Securely deleted and destroyed
Legal costs	Current year + 5	Securely deleted and destroyed
Invoices	Current year + 5	Securely deleted and destroyed
Orders placed for items	Current year + 5	Securely deleted and destroyed
Company purchase records	Current tax year + 5	Securely deleted and destroyed

Document description - Finance	Retention period - Years	Action following retention
Company insurance policies	Until renewed+5 years	Securely deleted

		and destroyed
Employee liability claims	Permanent	

Document description - ICT	Retention period - Years	Action following retention
Operating logs	Active + 1 rolling	Archived
Security incident reports	Current year + 5	Securely deleted and destroyed
Emails	Active + 1 rolling	Archived, Securly deleted
Business continuity plan	Active	

Document description - Health	Retention period - Years	Action following retention
Health and safety records	Current year + 5	Securely deleted and destroyed

Document description – Participants - child	Retention period - Years	Action following retention
Name, Current address details, telephone number/mobile number/ personal email address	Current + 2	Pseudoanonymised on Upshot
Date of birth, gender,	Current + 2	Pseudoanonymised on Upshot
Special Data-Medical needs/disability, ethnicity	Current + 2	Pseudoanonymised on Upshot
Current school name	Current + 2	Pseudoanonymised on Upshot
Case Study Data	Current + 5	Deletion of Data plus Anonymised for analytical purpose

Document description – Participant – vulnerable adult	Retention period - Years	Action following retention
Name, Current address details, telephone number/mobile number/ personal email address	Current + 2	Pseudoanonymised on Upshot
Date of birth, gender,	Current + 2	Pseudoanonymised on Upshot
Special Data-Medical needs/disability, ethnicity	Current + 2	Pseudoanonymised on Upshot
school	Current + 2	Pseudoanonymised on Upshot
Personal story (case study – do I need to describe this it will be as above plus a range of details to illustrate their story?)	Current + 5	Deletion of Data plus Anonymised for analytical purpose

Document description – Volunteers and unpaid coaches (Programmes)	Retention period - Years
Name, Current address details, telephone number/mobile number/ personal email address	Current + 2 Pseudo. As above
Date of birth, gender	Current + 2 Pseudo. As above
Personal story (case study – do I need to describe this it will be as above plus a range of details to illustrate their story?)	Current + 5 Anonymised. Deletion of Data plus anonymised for analytical purpose

Name, Current address details, telephone number/mobile number/ personal email address	Retain for current staff. Former staff Termination + 2
DBS and training/certification	Retain for current staff. Former staff Termination + 2

Document description – Employed coaches	Retention period - Years

Name, Current address details, telephone number/mobile number/ personal email address	Retain for current staff. Former staff Termination + 2
DBS and training/certification	Retain for current staff. Former staff Termination + 2

Document description - Membership	Retention period - Years
Name, Current address details, telephone number/mobile number, email address provided by member, DoB, gender	Life of membership plus 6 years
Bank Details for Direct Debit collection of membership	Life of use of details
Application Form	Life of membership plus 6 years

Document description – Event Attendees/Participants	Retention period - Years
Name, Current address details, telephone number/mobile number/ personal email address	3 year after event / sign up – unless consent given
Special Data-Medical needs/Dietary requirements	1 Month after event
Challenge event Registrations	1 year after event – unless consent provided
Major Gift Donors	3 years after completion of project
Offline donors - I.e. cheques	1 year after event – unless consent provided
Legacy Donations –Gifts via wills	7 years after processed
Direct debit – cancellation of regular gift	Life of use
Prize Retention	2 years or until the prize is fulfilled