



SESSION RECORDING POLICY

Internal Policy — Ember Learning Ltd

Document Reference:	EL-SRP-002
Date Adopted:	1 September 2026
Status:	Adopted

1. POLICY STATEMENT

Ember Learning Ltd records all sessions delivered via its online platform ('Session Recordings'). Session Recordings are made exclusively for safeguarding purposes. They are not made for quality assurance, training, performance management, marketing, or any other purpose.

This Policy sets out how Session Recordings are made, stored, accessed, retained, and deleted. It applies to all Company staff, teachers, mentors, and any third party with any involvement in or access to Session Recordings.

This Policy is cross-referenced in and must be read alongside:

The Child Protection and Safeguarding Policy

The Online Safety Policy

The Data Processing Agreement (EL-DPA-001)

The Teacher and Mentor Agreement (EL-TMA-SE-003A or EL-TMA-E-003B)

Any individual who has access to, or responsibilities in relation to, Session Recordings must read and comply with this Policy.

2. PURPOSE OF SESSION RECORDINGS

2.1 Session Recordings are made for the sole purpose of enabling safeguarding reviews. Specifically, Recordings may be reviewed if:

A safeguarding concern is raised or identified in connection with a Session

A teacher's or mentor's conduct during a Session is called into question

A Student or Mentee discloses information during a Session that may indicate abuse, neglect, or a risk to their welfare

A statutory body (such as the police or children's social care) requests access to a Recording as part of a lawful investigation

2.2 Session Recordings shall not be used for:

Quality assurance review of teacher or mentor performance

Curriculum development or training purposes

Marketing or promotional purposes

Research or data analysis

Any other purpose not explicitly set out in Clause 2.1

2.3 Any proposed use of Session Recordings beyond the purposes listed in Clause 2.1 requires prior written agreement with the commissioning body (as the Data Controller), whether that is a Local Authority, Multi-Academy Trust, private company or school and an assessment of the data protection implications under UK GDPR Article 5(1)(b) (purpose limitation).

3. LAWFUL BASIS FOR RECORDING

3.1 Session Recordings involve the processing of personal data (audio and video recordings of Students and Mentees of all ages served by the Company) and are therefore subject to the requirements of the UK General Data Protection Regulation and the Data Protection Act 2018.

3.2 The lawful basis for processing Session Recordings is:

Article 6(1)(c) UK GDPR — processing is necessary for compliance with a legal obligation (the Company's safeguarding obligations under the Children Act 2004 s.11 and, for individuals aged 18 or over, the Care Act 2014)

Article 6(1)(e) UK GDPR — processing is necessary for the performance of a task carried out in the public interest (the commissioning body's statutory duty to arrange alternative provision or mentoring, of which safeguarding is an integral part)

3.3 The commissioning body (Local Authority, Multi-Academy Trust, private company or school), as Data Controller, is responsible for ensuring that all necessary consent for Session Recordings is obtained prior to referring Student or Mentee to the Company, regardless of the individuals age. The Company does not hold this consent directly. Confirmation that consent has been obtained is a condition of the Service Agreement.

3.4 The Company includes information about Session Recordings in its standard Service Agreement and provides its Session Recording Policy to Commissioners on request, to support Commissioners in fulfilling their privacy notice obligations to parents and carers.

4. ACCESS CONTROLS

4.1 Access to Session Recordings is strictly limited to the following individuals:

Role	Name	Access Level
Designated Safeguarding Lead (DSL)	Jack Bradley	Full access — may view any Recording in connection with a safeguarding concern
Deputy Designated Safeguarding Lead	Mahesh De Zoysa	Full access in absence of DSL, or on DSL's instruction
statutory bodies (police,	As applicable	Access only where lawfully

children's social care, adult social care, LADO)		required or authorised — requires DSL authorisation and documentation
--	--	---

4.2 No other individual — including teachers, mentors, company staff other than those listed above, Company directors, Commissioners, parents, or carers — shall have access to Session Recordings, except where access is required by law and has been approved by the DSL.

4.3 Access permissions shall be reviewed by the DSL no less than annually to ensure they remain accurate. If a change of DSL or Deputy DSL occurs, access permissions shall be updated immediately.

4.4 Any request for access to a Session Recording — from any party — shall be directed to the DSL. The DSL shall assess the request, document the decision, and provide or refuse access accordingly. No Recording shall be shared without the DSL's documented authorisation.

5. STORAGE AND TECHNICAL SECURITY

5.1 Session Recordings shall be stored in encrypted, access-controlled storage. Full details of the storage solution in use, including data residency, encryption standards, and the Data Processing Agreement with the storage provider, are maintained in the Data Processing Agreement (EL-DPA-001) and updated whenever the storage solution changes. The DSL is responsible for confirming that the storage solution in use at any given time meets the requirements of this Policy.

The storage and platform arrangements in place at any given time are documented in the Data Processing Agreement (EL-DPA-001). Where the platform or storage solution changes, the DPA shall be updated and this Policy reviewed in accordance with Section 12.

5.2 The following technical and organisational security measures apply to Session Recordings:

Recordings are encrypted at rest using industry-standard encryption

Recordings are transmitted only over encrypted connections (HTTPS/TLS)

Access to Recording storage is protected by strong authentication (multi-factor authentication where technically supported)

Access logs are maintained and reviewed by the DSL periodically

No Recording is stored on any personal device or transferred to a personal email account under any circumstances

5.3 The DSL is responsible for ensuring that the storage solution used for Session Recordings meets the security standards described in Clause 5.2 and shall review technical security arrangements no less than annually.

5.4 Any actual or suspected unauthorised access to, or breach of security relating to, Session Recordings shall be treated as a Personal Data Breach and reported immediately to the DSL, who shall follow the breach notification procedure set out in the Data Processing Agreement.

6. RETENTION PERIOD

Session Recordings shall be retained for 6 months from the date of recording. If a safeguarding concern has been raised in respect of any session, the recording for that session must be retained for the duration of any investigation or legal proceedings and for a minimum of 8 years following their conclusion, or as directed by the relevant statutory authority, whichever is the longer. The chosen retention period must be communicated to Commissioners and referenced in the DPA.

6.1 Subject to Clause 6.2, Session Recordings shall be retained for a period of 6 months from the date on which the Recording was made.

6.2 Notwithstanding Clause 6.1, a Recording must be retained beyond the standard retention period where:

A safeguarding concern has been raised in respect of the Session to which the Recording relates — in which case the Recording shall be retained for the duration of any safeguarding investigation or proceedings, and for no less than eight (8) years following the conclusion of such investigation or proceedings

A statutory body has requested access to or retention of the Recording — in which case the Recording shall be retained in accordance with any applicable court order or lawful direction

Legal proceedings are anticipated or ongoing that may require the Recording as evidence

6.3 A record of all Recordings retained beyond their standard retention period, the reason for extended retention, and the anticipated end date of retention shall be maintained by the DSL.

7. DELETION PROCESS

7.1 At the end of the applicable retention period (as described in Clause 6), Session Recordings shall be permanently and securely deleted by the platform's automated deletion process, operating under the DSL's oversight. The DSL is responsible for confirming that the automated deletion process is functioning correctly and that recordings are deleted at the end of the applicable retention period.

7.2 Deletion shall be carried out using a method appropriate to the storage medium, ensuring that the Recording cannot be recovered after deletion.

7.3 A deletion log shall be maintained by the DSL, recording for each deleted Recording:

The session reference (date, subject, and group)

The date of deletion

The name of the individual who performed the deletion

Confirmation that deletion was complete

7.4 The deletion log shall be retained for five (5) years from the date of each entry.

7.5 On termination of a Commissioner's Service Agreement, all Session Recordings relating to that Commissioner's referred Students shall be deleted at the end of their applicable retention period and confirmation of deletion provided to the Commissioner in accordance with the DPA.

8. PROHIBITION ON UNAUTHORISED USE

8.1 No person shall access, view, copy, share, download, or use any Session Recording for any purpose not expressly authorised by this Policy.

8.2 Teachers and mentors are explicitly prohibited from making any independent recording of Sessions. This prohibition is set out in the Teacher and Mentor Agreement (EL-TMA-SE-003A or EL-TMA-E-003B, Clause 8.3) and the Confidentiality and Data Handling Undertaking (Schedule 2 of the Agreement). Breach of this prohibition constitutes a serious disciplinary and potential criminal matter.

8.3 Commissioners, Students, Mentees, parents, or carers do not have a right to access Session Recordings under this Policy. Requests for access from these parties shall be managed by the DSL in accordance with applicable data protection legislation and, if appropriate, referred to the commissioning Commissioner as Data Controller.

8.4 Any actual or suspected breach of this Section 8 shall be reported immediately to the DSL and treated as a serious matter, potentially engaging the Company's safeguarding procedures, data breach notification obligations, and if appropriate, referral to statutory authorities.

9. TRANSPARENCY AND COMMUNICATION

9.1 The existence of Session Recording is communicated to Commissioners in the Service Agreement and confirmed as a condition of referral.

9.2 Commissioners are responsible for informing parents and carers that Sessions are recorded for safeguarding purposes, and for obtaining appropriate consent prior to referral. The Company can provide a copy of this Policy to Commissioners on request to assist with this.

10. RECORDING FAILURE AND QUALITY ASSURANCE

10.1 RECORDING FAILURE PROTOCOL. In the event that a session is not captured by the approved platform recording function, the teacher or mentor must complete a written session log from memory immediately following the session. The log must include: the session date and time; students present; subjects covered; any behavioural or welfare observations; and a note that recording failed. The DSL shall log the incident for audit purposes.

10.2 MONTHLY DSL SPOT CHECK. The DSL shall conduct a monthly review of a sample of Session Recordings, excluding any recordings of sessions delivered by the DSL themselves. Sessions delivered by the DSL shall be reviewed by the Deputy DSL to confirm that recordings are capturing correctly and are accessible. The purpose of the spot check is operational assurance only — it is not a review of teacher or mentor performance or session content. A brief record of each spot check, including the date, sessions sampled, and any issues identified, shall be maintained by the DSL.

11. ROLES AND RESPONSIBILITIES

12. POLICY REVIEW

Role	Responsibility
------	----------------

Designated Safeguarding Lead (Jack Bradley)	Policy owner. Controls access to Recordings. Authorises any viewing or sharing of Recordings. Oversees deletion process and maintains deletion log. Reviews access permissions annually. Manages breach notifications.
Deputy DSL (Mahesh De Zoysa)	Acts in place of DSL when DSL is unavailable. Has the same access rights as DSL. Reports to DSL on return.
Company Director(s)	Responsible for ensuring adequate technical and storage infrastructure. Annual review of this Policy. No independent access to Session Recordings.
Teachers / Mentors	No access to Session Recordings. Must not make independent recordings. Must comply with Schedule 2 of the teacher Agreement.

This Policy shall be reviewed annually by the DSL, and following any of the following triggers:

A change in the platform or storage solution used for Session Recordings

A change of DSL or Deputy DSL

A Data Breach involving Session Recordings

A change in applicable data protection law or guidance

A significant change in the volume or nature of sessions delivered

The review date and policy version shall be updated below.

Policy Owner:	Jack Bradley, Director & Designated Safeguarding Lead
Date Adopted:	1 September 2026
Next Review Due:	1 September 2027 (or earlier if a trigger event occurs)
Approved by:	Jack Bradley, Director, 1 September 2026