SCREEN LMS

# Screen LMS Singapore Privacy Notice

Public notice describing Screen LMS personal-data purposes, disclosures, safeguards, retention, transfers and individual request channels.

**LEGAL AND ASSURANCE STATUS: Operational draft for implementation and UAT. It has not been represented as approved by Singapore-qualified counsel, an accredited certification body or an external auditor.**

| | | | |
|---|---|---|---|
| **Document code** | DP-001 | **Version** | 2.0 |
| **Effective date** | 2026-07-12 | **Next review** | 2027-07-12 |
| **Owner** | Data Chord Pte. Ltd. | **Audience** | all |
| **Status** | Pending review by Singapore-qualified counsel and the appointed DPO | **Acknowledgement** | Required for designated roles |

## Change history

| Version / effective date | Change | Owner | Approval status |
|---|---|---|---|
| 2.0 / 2026-07-12 | Material rewrite for Singapore PDPA, education-sector, transfer, breach, children and accountability requirements. | Data Chord Pte. Ltd. | Pending required approval and legal review |

Controlled copy: the current LMS-published version. Printed or forwarded copies are uncontrolled. A material change creates a new version; earlier versions and acceptance evidence are preserved.

## Purpose and scope

Public notice describing Screen LMS personal-data purposes, disclosures, safeguards, retention, transfers and individual request channels.

This document applies to Screen LMS application operations, relevant Azure services, authorised users, administrators, service providers and records within its stated audience.

## Governance principles

- Apply Singapore law, contractual commitments and approved organisational policy using documented, risk-based decisions.
- Use data minimisation, least privilege, separation of duties and secure defaults.
- Preserve evidence sufficient to demonstrate what was decided, implemented, tested and reviewed.
- Escalate uncertainty; do not treat this operational draft as legal advice or certification evidence by itself.

## Roles and responsibilities

- The document owner maintains this controlled version, monitors changes and initiates review after a material legal, technical, supplier or business change.
- Managers assign accountable control owners, approve resources and review significant exceptions, risks, incidents and overdue actions.
- Users and authorised suppliers follow the policy, complete required training, protect credentials and report suspected incidents or nonconformities promptly.
- The Data Protection Officer reviews personal-data implications and the security owner reviews confidentiality, integrity and availability implications.

## Who we are and how to contact us

Data Chord Pte. Ltd. operates Screen LMS. The production operator must publish the legal entity, appointed Data Protection Officer and monitored privacy-request channel in the LMS before production release.

## Personal data handled

Depending on role and enabled functions, Screen LMS may handle account and identity details, contact details, organisation and role assignments, enrolment and attendance, learning activity, assessment responses and grades, communications, support records, schedules, certificate records, payment references, device and security telemetry, audit events and user-supplied attachments.

## Purposes and legal bases

Screen LMS uses personal data to provide and secure the learning service, administer programmes and assessments, communicate operational information, issue and verify credentials, support users, meet contractual and legal duties, investigate misuse and improve service quality. Optional marketing is controlled separately and is not a condition of LMS access.

## Disclosure, processors and transfers

Data is disclosed only to authorised personnel, the relevant customer or educational organisation, approved service providers, professional advisers or public authorities where permitted or required. Overseas transfers require documented comparable protection, due diligence, contractual safeguards, location and subprocessor review, incident terms, return or deletion and an exit plan.

## Retention, security and incidents

Records are retained only for approved operational, educational, accreditation, legal, dispute and security purposes. Access is role- and tenant-scoped, transmission is protected, privileged activity is logged, backups are controlled and incidents follow the approved response process. A notifiable breach assessment is owned by the DPO and incident leadership.

## Access, correction and complaints

An individual may use the authenticated privacy-request route or the published DPO contact to request access or correction, subject to identity verification and applicable exceptions. The organisation records the request, provides status updates and explains any refusal or limitation. Complaints should first be raised through the published privacy channel.

## Data Protection Officer

Data Chord Pte. Ltd. must maintain and publish a monitored DPO contact channel. Production deployment must replace any placeholder contact information and document the accountable DPO appointment.

- DPO email: configured through the LMS environment and displayed in the policy centre.
- Privacy requests: accepted through the authenticated LMS form or published contact channel.
- Concerns may also be raised with the PDPC using its current official process after the organisation has had a reasonable opportunity to respond.

## Records and evidence

- Keep the approved version, superseded versions, approval record, publication record, acceptance evidence where required, training evidence, exceptions and review decisions.
- Apply role and tenant access restrictions, protect evidence from unauthorised change, and use the approved retention and secure-disposal schedule.
- Do not place secrets, passwords, access tokens or unnecessary personal data in governance evidence or issue trackers.

## Monitoring, exceptions and review

The owner reviews the policy at least by the scheduled date and after a material incident, audit finding, law change, supplier change, architecture change or significant processing change.

- Record each exception with business justification, affected assets or data, risk, compensating controls, approver, owner, expiry and review date.
- Track findings and overdue actions through the corrective-action process and verify effectiveness before closure.

- A material change creates a new controlled version. Where the policy is an access condition, the LMS presents the new version for renewed acceptance while preserving earlier evidence.

## Official sources and external references

Sources were checked during the 12 July 2026 policy refresh. The document owner must verify the current official version during every review. A source citation does not mean the issuing body has approved Screen LMS or this document.

- **Attorney-General's Chambers, Singapore: Personal Data Protection Act 2012 (Singapore Statutes Online)** — https://sso.agc.gov.sg/Act/PDPA2012
- **Attorney-General's Chambers, Singapore: Personal Data Protection Regulations 2021** — https://sso.agc.gov.sg/SL/PDPA2012-S63-2021
- **Personal Data Protection Commission: Data Protection Obligations** — https://www.pdpc.gov.sg/data-protection-obligations
- **Personal Data Protection Commission: Advisory Guidelines on Key Concepts in the PDPA (revised 29 April 2026)** — https://www.pdpc.gov.sg/organisations/regulations-decisions/regulatory-guidance/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act
- **Personal Data Protection Commission: Advisory Guidelines for the Education Sector (updated 25 April 2024)** — https://www.pdpc.gov.sg/organisations/regulations-decisions/regulatory-guidance/advisory-guidelines-for-the-education-sector
- **Personal Data Protection Commission: Guide to Cross-Border Data Transfers** — https://www.pdpc.gov.sg/organisations/resources/guidance-by-topic/guide-to-cross-border-data-transfers
- **Personal Data Protection Commission: Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment** — https://www.pdpc.gov.sg/organisations/regulations-decisions/regulatory-guidance/advisory-guidelines-on-the-pdpa-for-childrens-personal-data-in-the-digital-environment

## Approval and review record

| Role | Name | Decision / date | Notes |
|---|---|---|---|
| Document owner | To be completed | Pending | Required before representing this document as fully approved |
| Information security | To be completed | Pending | Required before representing this document as fully approved |
| Data Protection Officer | To be completed | Pending | Required before representing this document as fully approved |
| Singapore-qualified legal reviewer | To be completed | Pending | Required before representing this document as fully approved |