

SCREEN LMS

Biometric and Facial Photo Consent and Privacy Notice

Point-of-use notice and explicit consent terms for facial images and identity verification.

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	BIO-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	Notice / point-of-use control

Change history

Version / effective date	Change	Owner	Approval status
2.0 / 2026-07-12	Singapore legal, privacy, security and document-control refresh.	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

Point-of-use notice and explicit consent terms for facial images and identity verification.

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.

Point-of-use consent

This notice is presented immediately before the enabled workflow captures or uploads a facial reference photo. General acceptance of the privacy notice is not treated as biometric consent.

- State the purpose, data captured, method, recipients, retention and consequences of declining.
- Do not activate the camera or accept a photo until the explicit consent control is selected.
- Record the exact policy version, timestamp, user, source, IP address and policy digest.
- Provide a withdrawal route and explain that withdrawal does not require deletion where a lawful retention obligation applies.

Prohibited use

- Do not use facial information for unrelated marketing, emotion inference or general surveillance.
- Do not disclose the reference image to another learner or unauthorised staff member.
- Do not rely on a face-match score as the sole basis for a high-impact adverse decision without authorised human review.

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>
- **Personal Data Protection Commission: Guide on the Responsible Use of Biometric Data in Security Applications** — <https://www.pdpc.gov.sg/organisations/resources/guidance-by-topic/guide-on-the-responsible-use-of-biometric-data-in-security-applications>
- **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