SCREEN LMS

Screen LMS Acceptable Use Policy

Prohibits unauthorised access, abuse, harmful content, credential sharing, circumvention and unlawful use.

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	AUP-001	**Version**	1.0
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
1.0 / 2026-07-12	New Singapore-focused acceptable-use policy.	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

Prohibits unauthorised access, abuse, harmful content, credential sharing, circumvention and unlawful use.

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.

Permitted use

Use Screen LMS only for authorised learning, teaching, assessment, administration, support and approved research or testing. Follow instructions, data classifications and access boundaries.

Prohibited conduct

Do not share credentials, bypass controls, probe without written authority, impersonate another person, introduce malicious code, scrape restricted data, harass users, submit unlawful or harmful content, misuse assessment material or access another tenant's records.

AI and automated tools

Use generative or automated tools only where the programme and assessment rules permit. Do not disclose confidential or personal data to an unapproved tool, misrepresent generated work as original or automate access in a manner that harms availability or integrity.

Enforcement

The operator may preserve evidence, restrict access and investigate suspected misuse proportionately. Users receive a reason and review route where practicable. Serious conduct may be referred to the relevant organisation or authority.

Reporting

- Report suspected misuse through the support or security contact channel without probing beyond authorised access.
- Preserve relevant evidence and do not retaliate against a good-faith reporter.
- Security researchers must follow SECURITY.md and receive written authorisation before active testing.

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: Computer Misuse Act 1993** — https://sso.agc.gov.sg/Act/CMA1993
- **Attorney-General's Chambers, Singapore: Cybersecurity Act 2018** — https://sso.agc.gov.sg/Act/CA2018

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