AI, PRIVACY & DATA

Acceptable use & security awareness

Give users practical expectations for business technology, safe reporting and approved use of software and information.

DOCUMENT	PREPARED	STATUS
MSP-12	1 October 2026	Draft for adoption

Scope & application

Client users of managed devices, accounts, cloud services and approved AI tools. The client employer adopts workplace rules and gives appropriate notices about any monitoring.

Who does what

NovaSoft engagement lead

Scopes the work, assigns authorised personnel and maintains implementation and exception records.

Client service and risk owners

Approve access, business decisions, priorities, notices and residual risks; provide accurate scope and timely lifecycle requests.

Users and suppliers

Follow the approved arrangements, report issues and perform responsibilities assigned in the service schedule.

Draft for adoption. Confirm applicable requirements, implementation, owners and approval in the written client service schedule before operational use. Effective date is assigned on adoption.

THE POLICY IN PRACTICE

Control requirements.

01 Use authorised services

Use approved accounts, applications and licences for business activity. Do not bypass protective settings or connect unapproved tools to client data; request an assessment when a new tool is needed.

02 Protect account access

Keep credentials and recovery methods private. Use the approved password manager and MFA process; report unexpected prompts or suspected sharing through a known support route.

03 Handle messages carefully

Verify unusual requests, attachment sources and changes to payment or access details. Report suspicious activity without forwarding sensitive content widely or continuing to interact with a suspect link.

04 Respect information boundaries

Share business information only with authorised recipients and systems. Avoid personal storage, unapproved public AI and unverified transfer links for confidential material.

05 Report without delay

Provide a clear reporting route for lost devices, misdirected data and mistakes. Preserve useful context and let the response team coordinate containment rather than asking users to investigate or conceal a problem.

06 Make training practical

Include relevant guidance at induction and agreed refreshers. Adapt training for roles and accessibility needs. Simulation activity, monitoring and employment consequences require client approval and appropriate notice.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Client approves the acceptable-use rules and user notices.

02 Explain relevant practices at induction and role changes.

03 Provide accessible reporting and support instructions.

04 Review recurring questions and update practical guidance.

Agree with the client

- Permitted services and personal use
- User notices and training arrangements
- Simulation and monitoring authority
- Employer ownership of workplace decisions

Evidence to retain

- Adopted rules and notice records
- Training attendance and materials
- Reported issues and improvement actions

Exceptions & review

Record the requirement, reason, affected scope, risk owner, compensating measures and expiry or review date. Seek approval before deviating, or use documented emergency authority and arrange prompt review. Exceptions cannot waive applicable legal duties.

Review trigger: At agreed awareness refreshers, role changes and after relevant incidents or recurring errors.

Proposed owner: NovaSoft engagement lead with the client service/risk owner. Review at least annually, and earlier when the trigger above applies. Version changes require an approval and client-impact record.

References & related information

ASD/ACSC - Managed service provider guidance

OAIC - Privacy and commercially available AI

NovaSoft public policy library and application notes