
TECHNOLOGY AND INFORMATION POLICY

Technology, Internet, Email and Artificial Intelligence Policy

Using THRIV3 systems, and AI tools, responsibly and securely

Version 1.0 - July 2026

Policy owner	Board of Directors, THRIV3 (Indigenous Corporation)
Responsible officer	Chief Executive Officer
Applies to	Directors, members, the CEO, employees, volunteers, contractors, students on placement and agency workers of THRIV3 (together, THRIV3 People)
Effective date	July 2026
Next review	July 2027 (or earlier if legislation or funding conditions change)
Related documents	Privacy and Workplace Surveillance Policy; Social Media Policy; Code of Conduct

1. Purpose and Scope

THRIV3 (Indigenous Corporation) provides technology (THRIV3 Connectteam, the THRIV3 CMS, THRIV3 HR, the THRIV3 Risk Management App, email, devices, internet access and software) so our people can serve community effectively. This policy sets the rules for using THRIV3 technology and for using artificial intelligence (AI) tools in THRIV3 work.

It applies to all THRIV3 People who use THRIV3 systems, accounts, devices or data, on any device, anywhere.

2. Acceptable Use

- THRIV3 systems are provided for work purposes. Limited, reasonable personal use is permitted where it does not interfere with work, cost THRIV3 money or breach any policy.
- Protect your accounts: strong passwords, multi-factor authentication where available, lock devices when unattended, and never share credentials.
- Report suspected phishing, scams, malware or lost devices to your manager or to the CEO immediately.
- Take care with email: check recipients before sending, be professional in tone (emails are records), and do not open unexpected attachments or links.

3. Prohibited Use

Never use THRIV3 systems to create, access, store or send material that is unlawful, pornographic, discriminatory, harassing, bullying, defamatory or otherwise offensive; to download unauthorised software; to run a private business; to gamble; to infringe copyright; or to deliberately bypass security controls. Illegal material will be reported to the police.

4. Confidential Information and Data

Store THRIV3 information in THRIV3-approved systems, not personal accounts or personal cloud storage. Community, client, child-related and personal information receives the highest protection and is handled under the Privacy and Workplace Surveillance Policy. When your engagement ends, return all devices and data and do not retain copies.

5. Artificial Intelligence

AI tools (such as generative AI assistants) can improve how we work, and THRIV3 supports their responsible use within these rules.

Approved use

- Use AI tools approved by the CEO for THRIV3 work. If in doubt, ask before using a new tool.
- Good uses include drafting and editing documents, summarising public information, brainstorming, and preparing plans, provided a human reviews the output.

Non-negotiable rules

- **Never enter personal, sensitive, cultural, client, child-related, financial or confidential THRIV3 information into a public AI tool** that has not been approved for that data.
- **A human is always accountable.** AI output must be checked for accuracy, bias and cultural appropriateness before it is used or sent. You own what you send, whether or not AI helped write it.
- **Cultural knowledge is protected.** Do not use AI to generate First Nations cultural content, stories, artwork or language without cultural authority and CEO approval.
- **Decisions about people are made by people.** AI must not be used to make recruitment, disciplinary, funding or service decisions about individuals.
- Be transparent: where AI has materially produced content for external use, tell the CEO so appropriate review and disclosure can occur.

6. Monitoring

THRIV3 systems may be monitored in accordance with the Workplace Surveillance Act 2005 (NSW) and the Privacy and Workplace Surveillance Policy. Do not expect personal privacy in material created, stored or sent on THRIV3 systems.

7. Breaches and Review

Breaches may lead to withdrawal of system access, disciplinary action up to dismissal, or the end of an engagement, and serious matters may be reported to the police. The CEO maintains the approved software and AI tool list and reviews this policy annually.

Board adoption

This policy was adopted by the Board of Directors of THRIV3 (Indigenous Corporation) and takes effect from the date recorded below. It will be reviewed at least every 12 months, and earlier if legislation, ORIC or ACNC requirements, or funding conditions change.

Adopted On: 25/07/2026