HIVO

Digital Asset Management for AI-Ready Government Teams

Privacy-Ready Content Management Designed for Australian Government Organisations.

Disclaimer & Confidentiality Notice

The information contained in this document is confidential to the recipient and provided for general informational and marketing purposes only. It does not constitute legal, regulatory, or compliance advice and should not be relied upon as such. While HIVO has taken reasonable care to ensure the accuracy of the content, laws and regulations may change and the application of legal requirements will vary depending on the specific circumstances. You should seek independent legal or professional advice before relying on, or taking any action based on, the information provided herein. HIVO disclaims all liability for any loss or damage arising from reliance on the contents of this document.

Introduction to HIVO

Australian local governments and city councils capture thousands of photos, videos and documents, often featuring members of the public, children, staff and volunteers. With new privacy obligations already in force in Australia and increasing regulation yet to come, uncontrolled content libraries and ad-hoc sharing are a growing liability for local governments to manage.

HIVO is an Australian-founded, market leading ISO 27001-certified Digital Asset Management (DAM) platform hosted and operated right here in Australia. HIVO is built to help city councils govern content and personal information, manage compliance, and keep communication, content and legal teams moving forward.

Australia's privacy legal landscape is changing fast

The Privacy and Other Legislation Amendment Act 2024 (Cth) (POLA) received Royal Assent on 10 December 2024 and has given effect to a number of current and future changes aimed to enhance the privacy of individuals with respect to their personal information.

Government Clients Include

Bundaberg Regional Council · camden council · City of Stirling, City of Choice · City of Onkaparinga · Penrith City Council · AgriFutures Australia

Barwon Water · CrossRiverRail Delivery Authority · Fremantle Ports · MAPCO · Pilbara Ports · Queensland Hydro

ACT Government · Queensland Government · WA.gov.au · Government of Western Australia Department of Transport and Major Infrastructure · DFES Department of Fire & Emergency Services

TAFE NSW · Clean Energy Skills National Centre of Excellence · Public Transport Authority

Changes Required by POLA

Stronger security duties

The Privacy and Other Legislation Amendment Act 2024 (Cth) (POLA) strengthened Australian Privacy Principle (APP) 11, requiring councils and other organisations to do more than just take “reasonable steps” to protect personal information. You now must be able to demonstrate that both technical measures (such as encryption, multi-factor authentication, and secure hosting) and organisational measures (such as staff access controls and account deactivation when employees leave) are in place. The OAIC has been clear that compliance is no longer about intent alone—it requires a demonstrable security framework backed by evidence.

Real enforcement

POLA introduced a three-tier civil penalty regime. This includes not only the high-level penalties for serious or repeated breaches (already in the millions of dollars), but also mid-tier fines up to $3.3 million and low-tier infringement notices for what were once treated as administrative oversights - such as not having an adequate privacy policy or failing to provide a clear opt-out for marketing. The OAIC has also been given enhanced investigative powers, including the ability to issue public inquiries, meaning that reputational risk for councils is now much higher if privacy obligations are not met.

Greater transparency of automated decision making

From 10 December 2026, organisations will be required to clearly explain in their privacy policies any use of automated decision-making (ADM) that significantly affects individuals. For councils, this could apply to assets that are automatically saved into general 'approved for use' folders on a network drive, or general consent being relied on by signage alone. The OAIC has advised that transparency is key: people must be specifically told when automation plays a role in decisions and provided with an explanation they can understand. Councils that begin managing these practices now will be well-placed when the requirement becomes enforceable.

Individuals' privacy rights are strengthening

There is an increasing expectation under Australian law—and already under the GDPR and similar regimes globally—that individuals will have clear rights over their personal data. While a full right to erasure (the "right to be forgotten") is expected in a later tranche of reforms, POLA already reinforces the importance of consent, transparency, and deletion workflows. The OAIC expects consent to be voluntary, informed, current, and specific. Councils must be prepared to track where images or video of people appear, manage consent records, and act quickly if an individual changes or withdraws their consent or requests deletion.

Why General File Storage is No Longer Enough

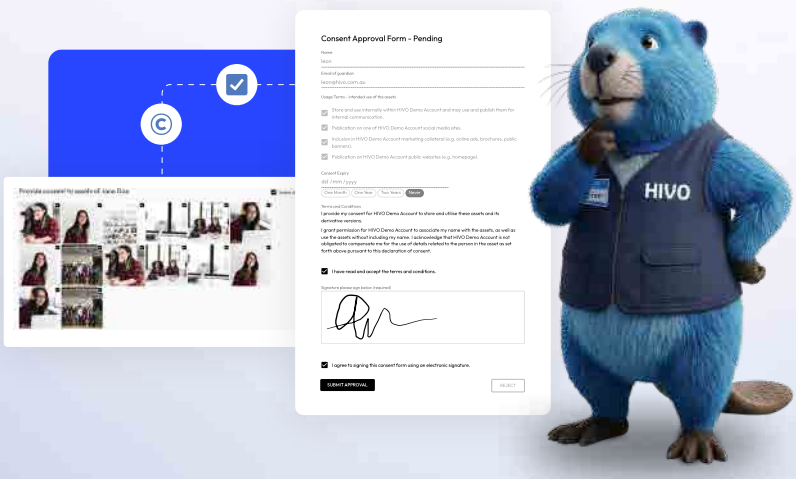
For years, councils have relied on general-purpose storage platforms - like SharePoint, Dropbox, Google Drive, or traditional network drives to hold community photographs, staff images, and multimedia content. While these systems are useful for everyday document management, they were never designed to govern sensitive and personal information such as images of members of the public, biometric identifiers, or consent-dependent media. As Australia's privacy obligations expand, the risks of relying on these tools are becoming aparent.

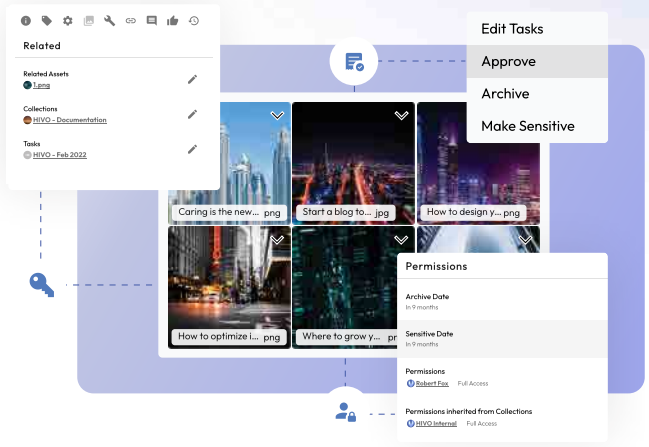
Lack of PII awareness and detection

Standard storage systems treat all files equally. They cannot automatically identify when a folder contains highly sensitive and personal data such as images of children at community events or staff records containing biometric identifiers. Without proactive detection, councils run the risk of inadvertently storing and sharing sensitive material in breach of APP 6 (Use and Disclosure) and APP 11 (Security of Personal Information).

Weak consent and usage controls

Dropbox, Google Drive, and network drives cannot link signed consent records to individual assets or attach Digital Rights Management workflows. A photo of a youth program participant without a signed consent form may be stored indefinitely without clear permission or a mechanism to revoke use. This gap creates non-compliance with APP 3 (Collection of Personal Information) and APP 5 (Notification of Collection), where the OAIC expects consent to be specific, current, and enforceable.





Over-sharing and permission creep

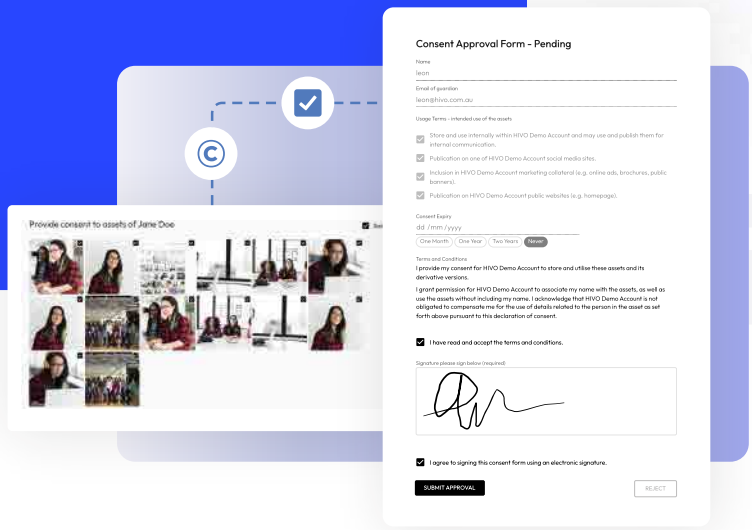
In general-purpose storage, access is often exclusively managed at the folder level. Over time, “permission creep” sets in: staff who no longer need access retain it, contractors or external users can gain broad rights, and files are downloaded or duplicated without audit. Councils then face the risk of privacy related content being disclosed far beyond its intended purpose—contravening the principles of data minimisation and proportionality.

No automated erasure or auditability

APP 11.2 requires personal information to be destroyed or de-identified once it is no longer needed. Traditional storage platforms lack the ability to search across libraries for an individuals data and bulk delete it with proof. They also provide limited, non-immutable audit trails, making it difficult for councils to demonstrate compliance in the event of an OAIC investigation.

Increased regulatory and reputational risk

With POLA 2024 introducing new infringement notice powers and a statutory tort for serious invasions of privacy, councils that cannot control the personal information they store of people risk both financial penalties and reputational damage. A single unauthorised disclosure of persons personal information could result in fines, loss of community trust, and negative media coverage. By contrast, the HIVO platform is fit for purpose to provide the controls missing from general-purpose storage: personal content detection, consent management, audit logging, role-based access, bulk deletion, and real-time policy enforcement. This ensures that councils meet the evolving expectations of the OAIC and build community confidence in how personal information is handled.



How HIVO helps Australian Councils

Consent Management Module

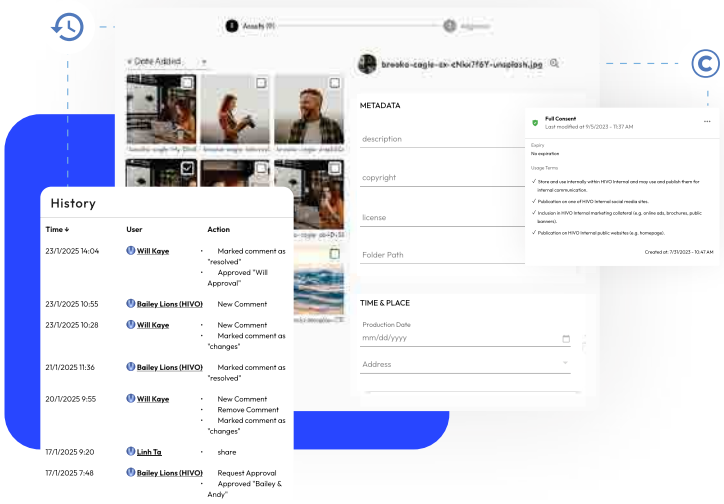
Councils can link digital consent forms directly to specific images or videos, record usage conditions (for example, “youth program only”), and handle consent revocations seamlessly. Consent becomes an enforceable, auditable part of the asset itself.

Personal Content Detection

HIVO’s Personal Content Manager automatically detects personal identifiers, including names, emails, faces and custom council-specific terms, classifying risk levels in minutes, not days. This gives councils immediate visibility over what personal information exists within their media libraries.

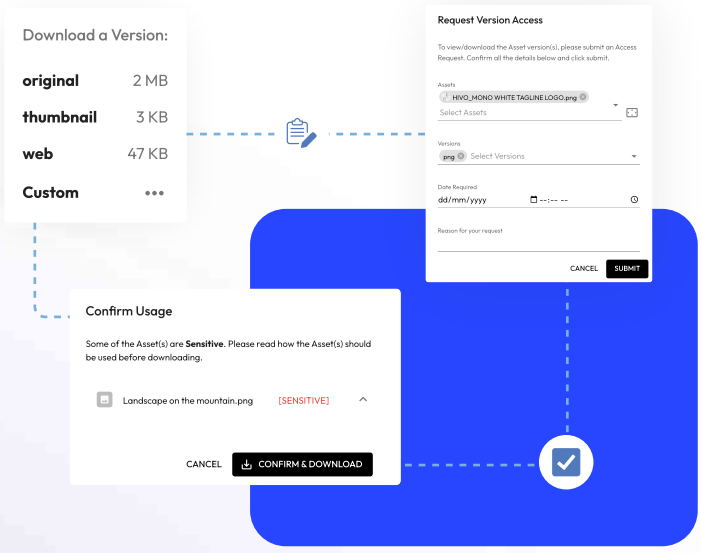
Audit Logging & Versioning

Every action on an asset (eg. upload, edit, approval, metadata, consent, deletion) is time-stamped and stored immutably. These logs can be exported for OAIC audits, internal risk reviews, or executive briefings.



Role-Based Access Controls (RBAC)

Access can be defined so that only the right staff—whether in Events, HR, or Communications—can view, share, or download personal or sensitive content. This supports OAIC's emphasis on organisational controls.

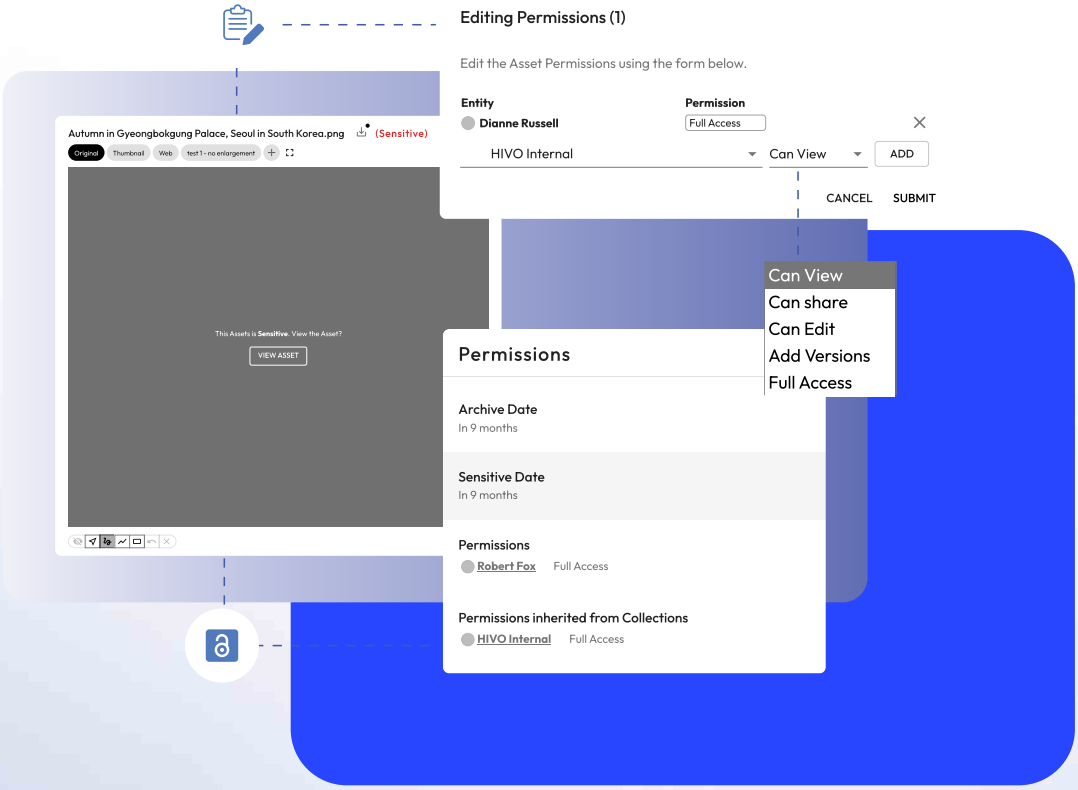


Bulk Edits & Deletion

If a resident requests erasure, councils can use HIVO's bulk tools to locate, edit, or delete all instances of their personal data across the entire library, with exportable proof of action.

Data Masking

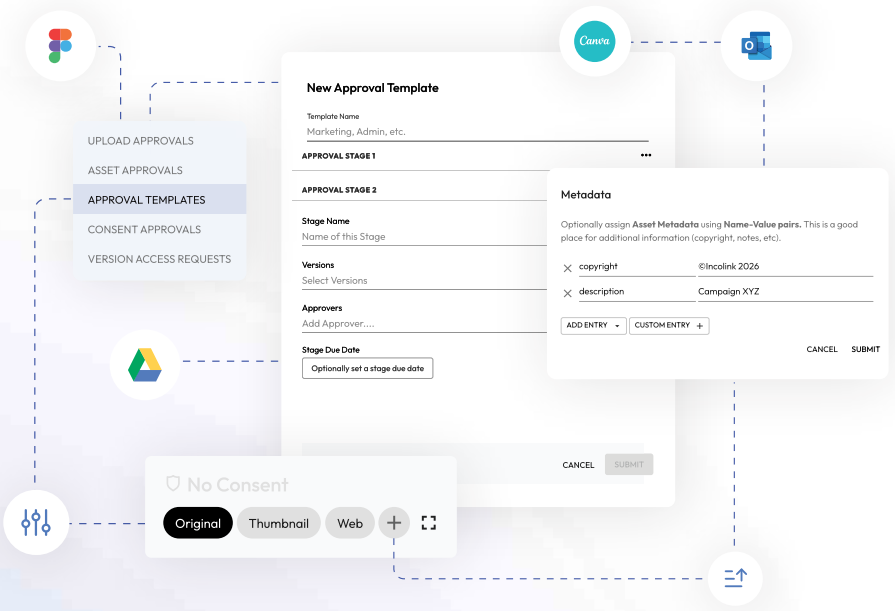
HIVO includes built-in data masking capabilities to protect sensitive or personal details without removing the underlying file. Councils can blur images, redact identifiers, or obscure personal fields in images and documents, enabling staff to work with content while reducing exposure of personal information. Masked copies remain linked to the original asset, ensuring flexibility for communications teams while maintaining compliance with OAIC guidance on minimising data handling risks.



How HIVO Can Help Councils Meet Their Record Keeping Requirements

HIVO addresses the complex retention demands of councils by mapping jurisdiction-specific schedules directly to configurable metadata fields and automated asset statuses. Councils can define retention periods, trigger events, and disposal workflows at the folder level. The latter ensures child folders (and the assets in them) inherit rules automatically while still allowing granular control over individual records. The platform's archive settings then move assets to cold storage based on predefined timelines, with administrators receiving notifications before destruction occurs. A recycle bin feature, which maintains deleted items for a specified period while audit logs track every action, provides additional oversight by creating a transparent evidence trail for compliance verification.

Beyond automation, HIVO builds accountability into retention processes through multi-step approval workflows. Records managers and asset owners work sequentially to review content before disposal, with the system displaying all metadata changes and edits for verification. Custom statuses such as archived, licence expired, or sensitive can be applied organisation-wide or to specific collections, each with distinct rules governing storage tiers and access restrictions. To prevent misclassification at the point of entry, upload approval mechanisms allow administrators to confirm that retention classifications match content types before assets enter the library. This combination of automated enforcement and human oversight helps councils maintain regulatory compliance while preserving operational flexibility.



Why Councils Choose HIVO

We know Australian councils use case

We work with over 100 government agencies and Australian city councils nationwide to help them better manage the privacy and compliance of content.

Australian-founded, Australian-hosted (AWS)

Data residency and local jurisdiction.

ISO 27001 certified

Independent assurance of security controls (visit our Trust Center at trust.hivo.co).

Integrated with the tools you use

Governed, central source of truth for media across all major software applications such as Microsoft and Adobe.

Local Australian support & onboarding

Practical rollout for communications, legal, IT and content teams.

Provider Comparison - Client Data Storage Location

HIVO

HIVO is an Australian company committed to safeguarding the data that we process and store on behalf of our clients. We store all client data, including client personally identifying information (PII) records on secure AWS servers (including sub processors and data backups) located in Sydney.

bynder

Bynder's client data will be hosted on AWS in a non-Australian regions:

- ap-northeast-1 (S3 server in Asia Pacific, Tokyo)
- eu-central-1 (S3 server in EU, Frankfurt)
- us-east-1 (S3 server in US East - North Virginia)
- us-west-1 (S3 server in US West - California)

Source: https://support.bynder.com/hc/en-us/articles/360013934099-Where-does-Bynder-Store-Assets

Canto

All Canto client data resides on AWS regions around the US, EU, and Canada. Currently, data is hosted in the following regions:

- Ireland
- Germany
- US West
- Canada Central

Source: https://www.canto.com/features/security/

Common Use Cases for Councils

Community & Events

Appropriately govern event photography and videos featuring residents and minors.

Corporate Affairs & Media

Rapid, compliant asset distribution to staff, councillors and media partners.

Libraries, Arts & Heritage

Manage archival images with consent records and clear usage restrictions over licensing and copyright.

Parks & Recreation / Youth Programs

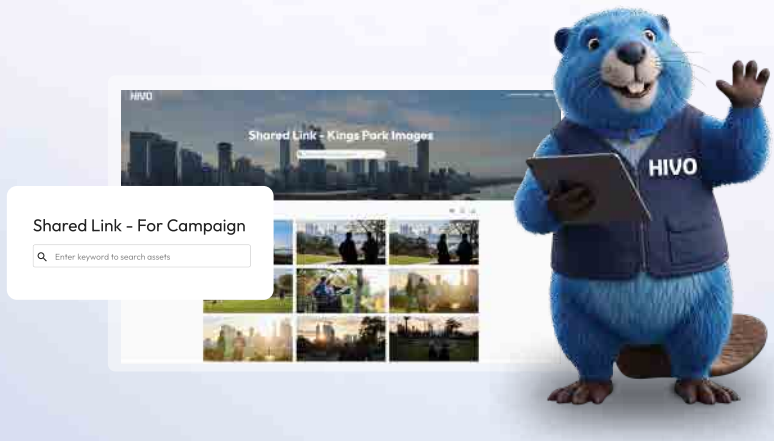
Separate, security-trimmed workspaces for program leads.

People & Culture (HR)

Personal staff images and documents kept private with roll based access control and auditability.

Legal Compliance

Set custom terms and conditions and application configurations based on business and privacy policies.



Example Rollout Plan

Days 1–30: Foundations & Visibility

Kick-off workshop with Comms, IT, and Privacy Officer to align goals and scope.

Baseline audit of current photo/video libraries, shared drives, and cloud folders.

Deploy PII scanning rulesets faces, identifiers, terms and local business specific rules.

Enable owner workspaces for departments (Admin, Events, Legal, HR, Communications).

Initial Personal Content Analysis Report delivered to council privacy lead.

Outcome Clear view of where privacy related content lives and who manages it.

Days 31–60: Protection & Compliance in Action

Activate real-time content shield on high-risk libraries (Comms, Events, Youth, HR).

Roll out Consent Management Module with digital consent forms linked to assets.

Train department leads on reviewing and approving quarantined content.

Rehearse erasure & correction requests using bulk deletion and metadata scrubbing.

Publish draft consent terms and notices informed consent, specific usage purposes, plain language, localised to be council specific.

Outcome privacy content automatically detected and quarantined; consent and deletion processes tested end-to-end.

Days 61–90: Optimisation & Reporting

Embed Privacy Impact Assessment (PIA) playbook for high-risk uses (facial recognition, AI tagging, storage of signed release forms).

Launch compliance dashboards for Privacy Officer and executive reporting.

Finalise privacy notices and consent templates for staff and contractors.

Quarterly audit exports scheduled for ongoing assurance.

Board/Executive briefing pack provided, demonstrating compliance readiness.

Outcome sustainable, auditable governance framework with regular reporting and executive visibility.

What success looks like

Fewer incidents from uncontrolled sharing or legacy drives.

Faster responses to privacy requests (days → hours).

Clear accountability with who-did-what-when logs.

Confident publishing with approvals and usage rights enforced.

Book a demo at hivo.co

Live PII detection and quarantine
Consent workflows linked to images and videos that contain people
Reporting pack for your privacy officer and compliance teams

1300 93 6564 info@hivo.co hivo.co