pps

FOR PROFESSIONALS

SINCE 1941

Trust First: Governing AI in a Mutual Environment

Early insights and emerging considerations

6 May 2026

Agenda

About Professionals Provident Society (PPS)

South Africa's only mutual financial services company for graduate professionals.

AI in the Workplace | People, Lifecycle & Literacy *(Masenyane Molefe, Group Executive: HR)*

- **AI in the Workplace |** The reality of AI adoption, what leadership sees versus what is really happening, and the gap between approved and informal AI use.
- **The Employee Lifecycle & AI |** Examples of where AI is already influencing decisions in HR
- **AI Training & Literacy |** Role-based AI literacy framework and why literacy is the foundation for governance.

Governing AI | Strategy, Structure & Lessons Learned *(Leenesh Singh, Senior Manager: Digital Innovation and Transformation)*

- **Managing AI: 5 Strategic Options |** Overview of five strategic approaches to AI governance, from open experimentation to governed enablement.
- **The PPS AI Governance Council |** The AIGC model, structure, AI Register, risk tiering, and the end-to-end governance process.
- **External Review |** What PPS got right and what needs to be strengthened based on external assessment findings.

About PPS

1941

Founded in 1941, PPS is the only mutual financial services company in South Africa that focuses exclusively on graduate professionals

4-year degree to qualify as a PPS Member

Mutual: All profits generated through PPS operations, are paid back to members. Unlike other Insurers where profits go externally to shareholders, PPS members are regarded as shareholders
140,000 Members. R6.88 billion ($410 million) in Profit-Share allocated in 2025

Comprehensive suite of financial solutions: including life insurance, short-term insurance, investments and medical aid

Since we do not have shareholders, products are designed for purpose, not profit. Our Products provide unmatched value and benefit

www.pps.co.za

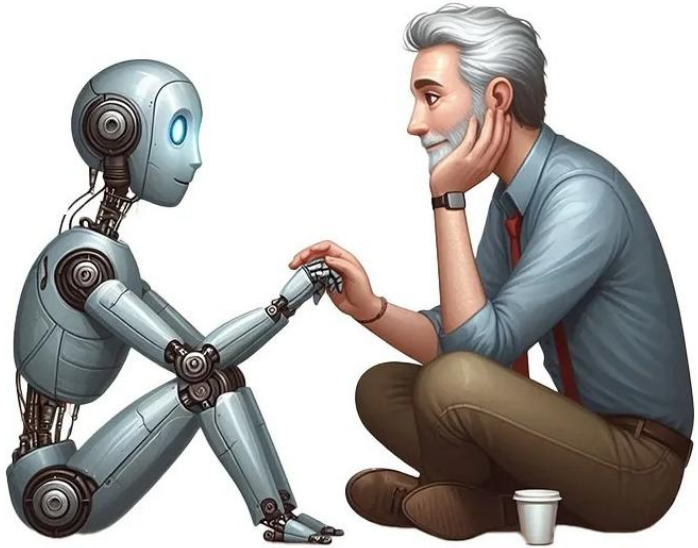
AI in the Workplace

People, Lifecycle & Literacy

AI in the Workplace | The Reality We All Face

AI is already in the workplace

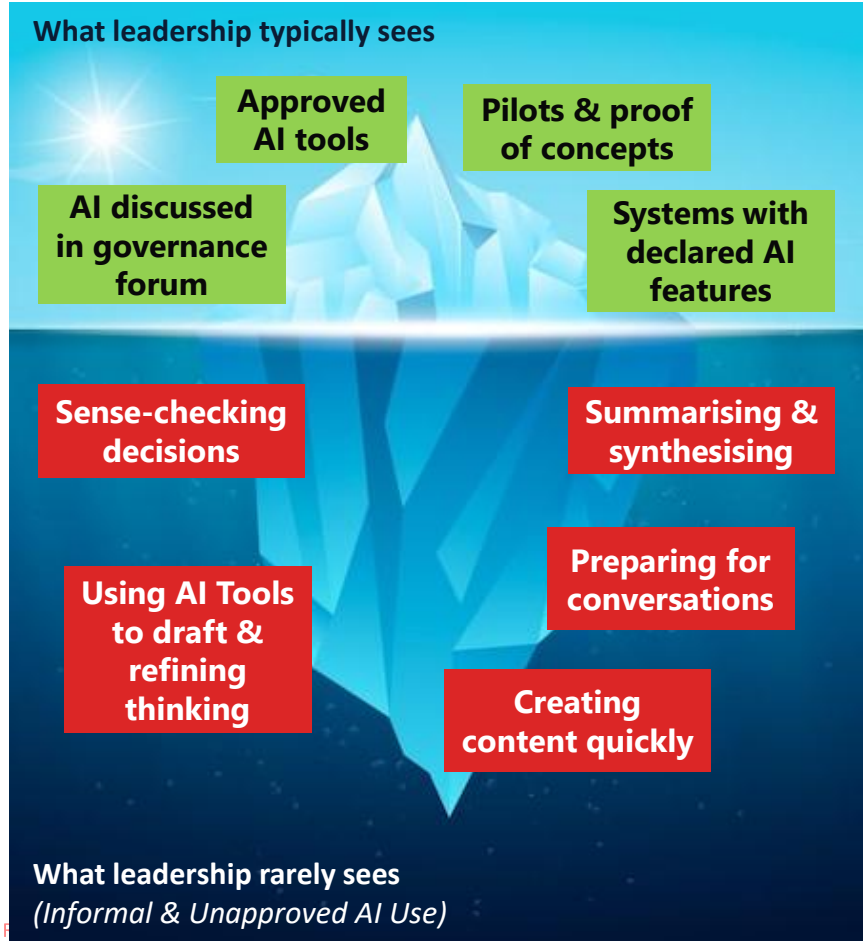
Staff are experimenting with tools independently



If there is an easier way to achieve an outcome, people will use it.

AI lowers effort, reduces friction, and speeds up work. That makes it naturally attractive to employees and managers.

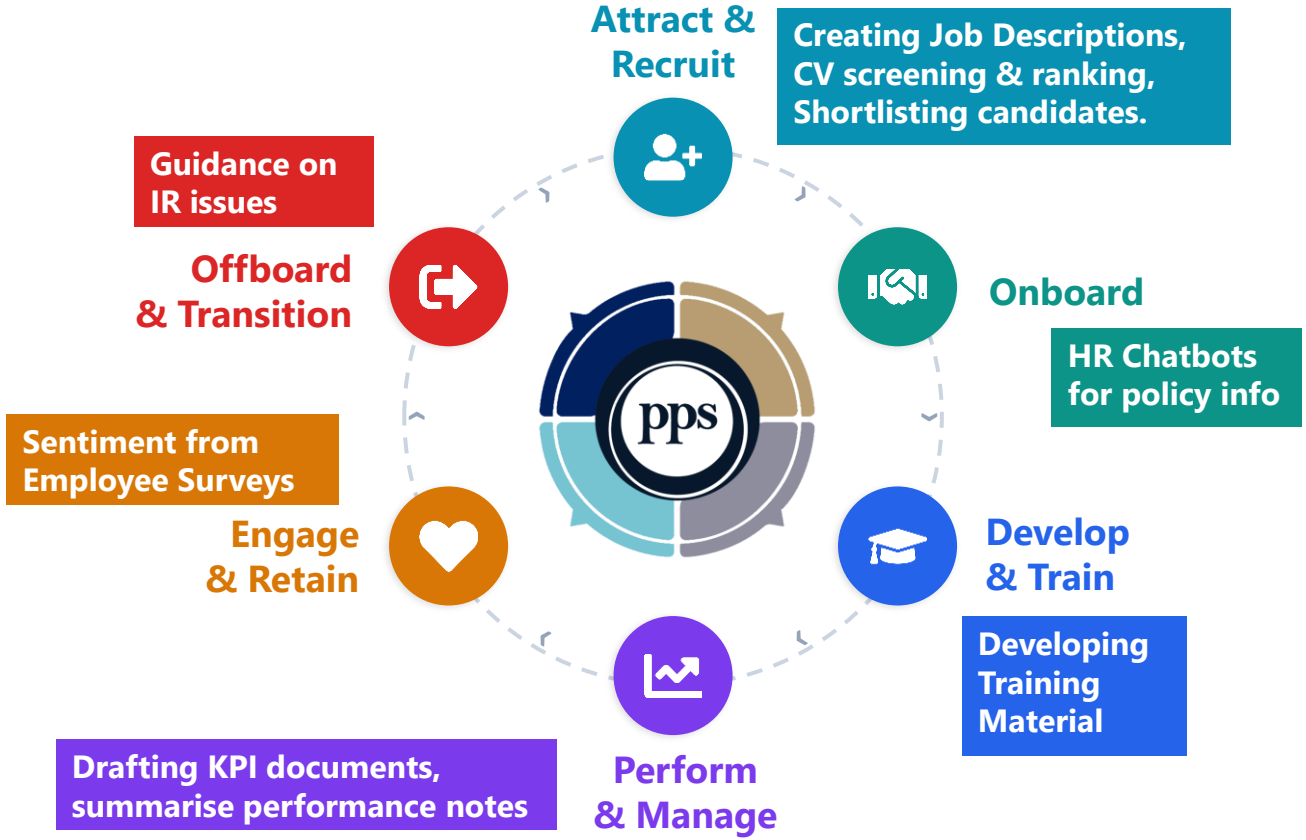
AI in the Workplace | What we see versus what is really happening



Individually, these feel low-risk. Collectively, they influence judgement and outcomes.

Global research shows nearly half of employees admit to using AI tools without formal approval, often sharing sensitive data [cio.com]

The Employee Lifecycle | Some Examples where AI Is Already Used



AI is already influencing decisions.

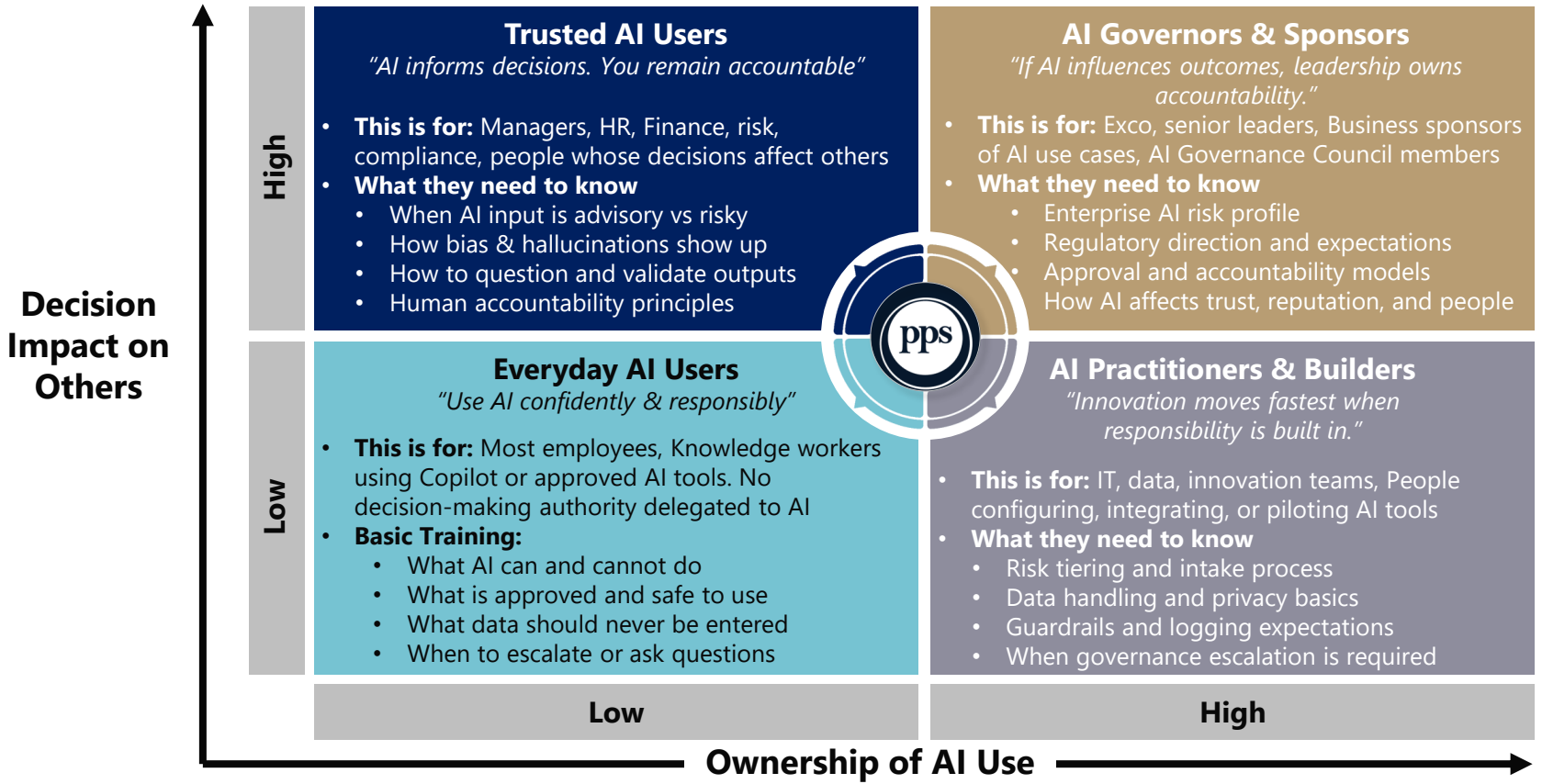
Even "minor" uses of AI still shift judgement from people to systems.

These decisions are happening quietly, incrementally, and without formal oversight

Different roles interact with AI differently. That requires different levels of AI literacy.

AI Training | Role-based AI literacy

Not everyone needs the same AI training, but everyone needs the right training.



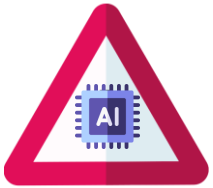
AI Literacy is the Foundation | Governance Is the Next Step

AI literacy is about understanding risk and judgement

Our goal was AI literacy, not expertise (such as coding).

People needed to:

- Understand what AI can and cannot do
- Apply judgement and challenge outputs
- Know when to pause or escalate



But literacy alone does not manage enterprise risk.

What literacy does not solve:

- Inconsistent decisions
- Unclear accountability
- No escalation path
- No single source of truth

Governing AI

Strategy, Structure & Lessons Learned

Managing AI | 5 Strategic Options

	 **Allow Uncontrolled Experimentation** Organizations allow employees to use any AI tools they choose without formal training or governance.	 **Block AI (Complete Prohibition)** Banning public AI tools (like ChatGPT, Claude) on corporate devices & networks	 **Sanctioned Enterprise Grade AI** The organisation provides employees with vetted, secure AI platforms such as Microsoft Co-Pilot	 **Sandboxed Experimentation (Controlled)** providing a secure, isolated environment for testing AI models	 **Governed Enablement** Establishing a formal framework of policies, training, and ethical guidelines
Risk Level	HIGH	LOW	LOW	MEDIUM	LOW
Productivity Gain	MEDIUM	NONE	HIGH	MEDIUM	VERY HIGH
Implementation Effort	NONE	LOW	HIGH	MEDIUM	VERY HIGH
	High **innovation** speed but risks **IP leakage** and regulatory breaches.	**Stops data leaks** but drives employees toward **"Shadow AI".**	Secure and **highly productive**, but requires significant **budget** and vendor vetting.	**Safe testing** environment, but isolated results can be hard to **scale to production.**	The **"Gold Standard"** maximizes ROI through policy, training, and secure tools.

AIGC | The PPS AI Governance Council Model

 **Started the AI Council Name: AIGC**	 **Structure & Composition**	 **AI Register (Inventory)**	 **Risk Tiering**
Slogan: Advancing Mutuality Through Responsible and Innovative AI Governance	**AI governance only works when it is shared.**	**Single Source of Truth**	**Right controls, not blanket control**
• Clear Terms of Reference (TOR) • Clear purpose. Why the council exists • Defined scope. Which AI use cases and systems it governs • Defined authority. What can be approved or stopped • Clear roles & responsibilities. Who does what • Explicit decision rights. What decisions sit where	• Operates under an Exco mandate • Deliberately cross functional by design • HR, Legal, Risk, Security, Architecture, Data and functions all represented • Ensures decisions are made early, not blocked late • Prevents fragmented AI decisions across silos	• Central register of all AI use cases, tools and models • Every AI use case has a named business owner • Accountability cannot be delegated to vendors • Links to risk tier, approvals, controls and evidence • Feeds the AI App Store / catalogue: Simple principle. If it is in the catalogue, staff can use it with confidence	• Green. Safe to experiment within guardrails • Amber. Allowed with guided oversight and controls • Red. Formal approval required before use • Risk tier considers data sensitivity, customer impact, automation level and regulatory exposure

AIGC on a Page | Your road to Responsible and Innovative AI Governance

Working on a new AI initiative?

Log it on the AI Register

There is a Fast Track Option for Tier 2 & 3 only, but requires business justification

Architecture & Security receives a notification of a new item logged

Everything is logged! What counts as "AI"?: Chatbots, copilots, and virtual assistants, machine-learning models and decision engines, AI-generated recommendations, summaries, or prioritisation, AI tools

AI Office

- Manages AI Registry
- Manages AI Catalogue

Enterprise Architecture

Architecture provides the following:

- Conducts the initial assessment & Allocates a Risk Tier
- Refers to IT Security if required
- Makes a recommendation to AIGC on how to proceed

- **Tier 1 (High Risk):** Sensitive data, financial decisions, etc
- **Tier 2 (Medium Risk):** Decision support with human override
- **Tier 3 (Low Risk):** Internal productivity tools

IT Security, Risk & Governance

- Evaluate risk, ethics, fairness & compliance.
- Human-in-loop needs
- Privacy/data sensitivity
- Compliance
- Unintended consequences
- Security & resilience
- Ongoing Scanning

AI Governance Council (AIGC)

- **Makes final decisions: Go / No-Go / Remediate / Sandboxed**
- Monitors Evidence & accountability
- Ongoing Audit Reports (breaches, hallucinations, data leak, etc)

AI Office

- Update AI Catalogue

Enterprise Architecture

Governance, Risk & Security

AIGC

AI Office

External Review | What We Got Right vs What We Need to Improve

What We Are Doing Right

- ✓ **Established early AI Governance**
- ✓ **Composition of AI Council is balanced**
- ✓ **Maintain an AI inventory:**
- ✓ **Risk Based Controls (Tier 1, 2, 3)**

What we need to strengthen

1. **Monitoring and Auditing (clarity and evidence)**
   - What do we watch continuously versus what we formally review and evidence.
   - Prove end-to-end AI monitoring coverage
   - Produce logs, dashboards, and records that show controls are working in practice.
2. **Accaccountability and Ownership**
   - Make accountability explicit, with IT owning technical controls and the business owning outcomes, cost, and residual risk.
3. **Risk Standards and Re-assessment**
   - Set minimum standards for bias, quality, and hallucination checks
   - Formalise re-assessment triggers, clearly stating when AI must be reviewed again due to changes.
4. **Vendor and Contract Controls**
   - Strengthen baseline contract and DPA requirements for AI vendors, covering data use & deletion