apex

Computing Services

make IT simple

Shadow AI Action Plan for Leaders

ARTIFICIAL INTELLIGENCE

What Is Shadow AI?

Shadow AI refers to any AI usage that occurs outside of approved organisational tools, policies, or governance.

Common examples include:

- Employees using public AI tools or free accounts to write client emails
- Teams uploading documents into unapproved platforms
- Staff using personal accounts to access AI assistants
- Departments adopting AI tools independently without IT visibility

The risk is not AI itself - it is uncontrolled AI use without guardrails.

Why Blocking AI Isn't The Answer

A common first reaction is to block public AI tools entirely. While this may reduce surface-level exposure, it rarely solves the underlying issue, often leading to:

- Workarounds using personal devices or accounts
- Reduced transparency and openness
- AI usage becoming harder to detect
- Productivity frustrations across teams

The safer approach is:

✓ Visibility
✓ Policy
✓ Approved tools
✓ Education
✓ Governance

Shadow AI is best addressed through enablement, not suppression.

Executive Summary

AI tools are now part of everyday work. Employees are using them to draft emails, summarise meetings, analyse data, and generate content - often without formal guidance or oversight.

This is known as Shadow AI: the use of AI tools that have not been formally approved, governed, or monitored by the organisation.

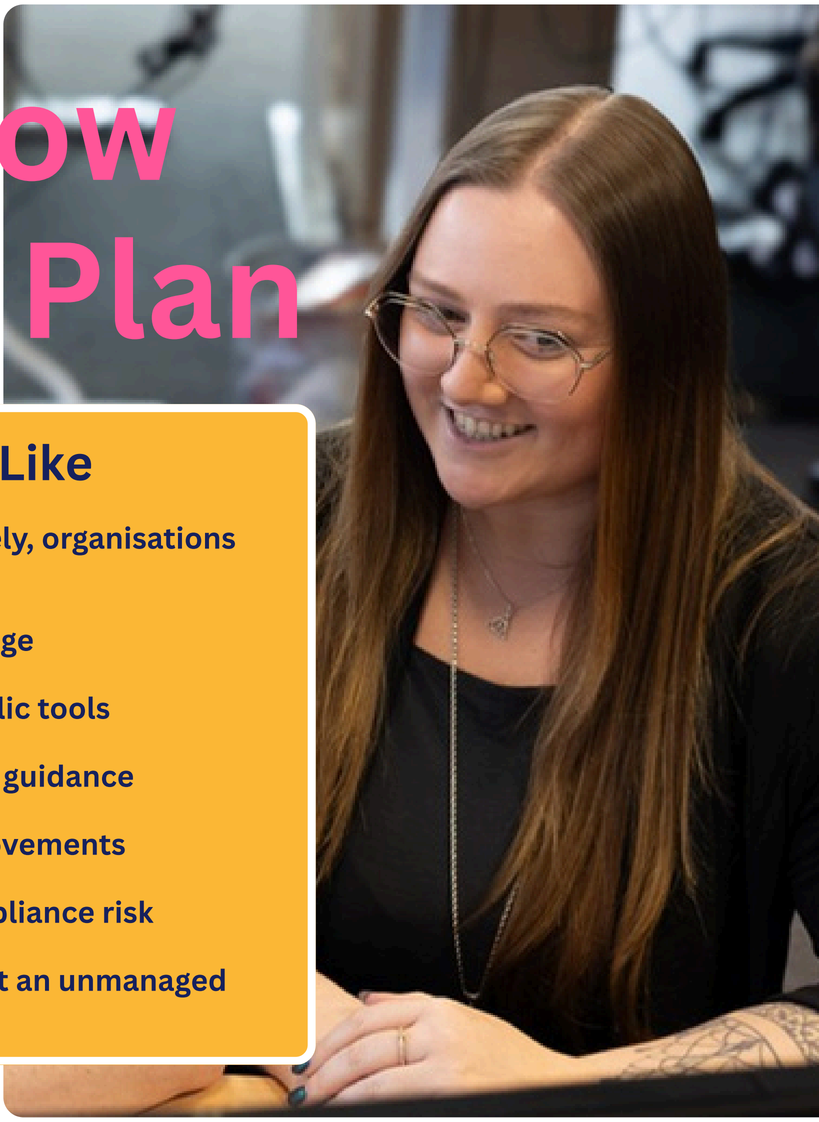
Shadow AI is rarely driven by bad intent. In most cases, it's a natural response to increasing workload pressure and the accessibility of public AI tools.

The challenge for organisations is clear:

How do you enable the benefits of AI without introducing uncontrolled risk?

This Action Plan provides a structured approach to reducing Shadow AI exposure while supporting safe, production adoption.

The Shadow AI Action Plan



What Good Looks Like

When Shadow AI is addresses effectively, organisations achieve:

- Visibility into AI usage
- Reduced reliance on public tools
- Clear staff confidence and guidance
- Secure productivity improvements
- Lower operational and compliance risk

AI becomes a business advantage - not an unmanaged exposure.

1 Step 1: Acknowledge AI Is Already Happening

The first step is recognising that AI adoption is not a future event - it is already occurring across most organisations.

Leaders should assume:

- Employees are experimenting with AI
- Usage is uneven aceoss departments
- Some may involve sensitive data
- Most people are unsure what is “allowed”

The goal is to bring AI into the open

2 Step 2: Start with Conversations, Not Controls

Before introducing restrictions or policies, begin with open discussions.

Ask teams:

- Are you using AI tools today?
- What tasks are you using them for?
- Where are you unsure what’s safe?
- What would help you use AI responsibly?

These conversations build trust and provide visibility.

Shadow AI is rarely a people problem - it’s a clarity problem

3 Step 3: Assess Your Current Risk Level

You cannot manage what you cannot see.

A simple Shadow AI risk review should focus on:

- What AI tools are being used
- What types of data may be shared
- Whether approved alternatives exist
- Whether staff understand safe usage

Many organisations begin with a short internal assessment or quiz to establish a baseline.

Outcome: A clearer picture of urgency and exposure

5 Step 5: Provide an Approved, Secure AI Alternative

Shadow AI thrives when employees have no safe option.

If teams are blocked from AI tools without an alternative, usage will simply move underground.

Secure, business-grade AI tools (such as Microsoft Copilot) provide:

- Data protection within your environment
- Permission-based access
- Compliance alignment
- Integration into existing workflows

The goal is to enable productivity safely, not remove capability

4 Step 4: Define What "Safe AI Use" Means for Your Business

Organisations need clear boundaries, not lengthy documents.

A practical AI usage policy should answer:

- What data should never be entered into AI tools? *(Client data, financial information, employee records)*
- Which tools are approved for business use?
- When is human review required?
- Who owns AI governance internally?

Policies should be short, clear, and accessible

6 Step 6: Educate Teams with Practical Guidance

Policies alone are not enough. Staff need real-world understanding.

Effective education includes:

- What AI is good for (and what it isn't)
- What information is safe to use
- Examples of approved use cases
- How to ask better questions (prompting)
- When to escalate uncertainty

Education reduced risk more effectively than enforcement

7 Step 7: Introduce Governance Without Slowing Innovation

Governance doesn't need to be heavy.

A proportionate approach includes:

- Approved tools list
- Light-touch review for new AI adoption
- Department champions or owners
- Periodic usage check-ins
- Clear escalation routes

Good governance supports AI progress rather than blocking it

9 Step 9: Monitor, Review, and Adapt

AI evolves quickly. Shadow AI risk is not a one-time issue.

Leaders should review:

- How AI usage is changing
- Whether staff feel supported
- Whether policies remain clear
- Whether new tools are emerging

Treat AI as an ongoing capability, not a one-off project

8 Step 8: Focus on High-Value, Low-Risk Use Cases First

The safest way to adopt AI is to start with common, low-risk productivity wins:

- Summarising internal documents
- Drafting non-sensitive communications
- Meeting notes and action tracking
- Internal reporting support
- Knowledge base creation

Early wins build confidence and create momentum

Your Next Steps

If your organisation is beginning this journey, start here:

Run a Shadow AI Risk Check

Open conversations with teams

Define safe boundaries

✓ Provide approved tools

Build confidence through education

You do not need to solve everything at one - but you do need to start.

apex
Computing Services

make IT simple

How Apex Can Help

Apex supports organisations to adopt AI safely and effectively through:

- Shadow AI risk assessments
- Governance and Policy guidance
- Secure AI enablement with Microsoft Copilot
- Practical use-case frameworks
- Ongoing support and education

Visit: **www.apexcomputing.co.uk**

Email: **enquiries@apexcomputing.co.uk**

Call: **0161 233 0099**

Let’s future-proof your business together.