# AI Risk & Responsibility Guide

## A Companion Guide to the Calder IT AI Factsheet & Readiness Checklist

Artificial Intelligence is rapidly becoming embedded within everyday business operations. This guide expands on the six key risks highlighted in the Calder IT AI Factsheet and provides practical governance guidance for organisations looking to adopt AI safely, securely and responsibly.

**Key Message**
The objective is not to avoid AI. It is to ensure AI is used safely, securely and responsibly across the organisation.

## 1. Misinformation & Inaccurate Outputs

### The Risk

AI systems generate responses by predicting likely content rather than understanding information in the way a human expert does. While results often appear professional and authoritative, they can contain factual errors, outdated information or fabricated references.

### Why It Matters

Many organisations are using AI to draft reports, policies, customer communications and research summaries. If content is accepted without verification, poor information can quickly spread through an organisation.

**Business Impact**
Poor business decisions; customer misinformation; compliance issues; reputational damage.

**Calder IT Recommendation**
Human review should remain mandatory for important business communications and decisions.

**Key Takeaway**
AI can accelerate work, but accountability for accuracy must always remain with people.

## 2. Sensitive Data Exposure

### The Risk

Employees may unintentionally submit confidential information into AI platforms while seeking assistance. This can include customer data, contracts, employee records and commercially sensitive information.

### Why It Matters

Before approving any AI platform, organisations should understand where information is stored, retained and processed, and whether submitted information could be used to improve future models.

**Business Impact**
GDPR concerns; data loss; contractual issues; reputational damage.

**Calder IT Recommendation**
Provide clear rules on what information can and cannot be entered into AI tools.

**Key Takeaway**
Employees should never have to guess what information is safe to enter into AI systems.

## 3. AI-Assisted Cyber Threats

### The Risk

Cybercriminals increasingly use AI to create convincing phishing emails, impersonation messages and social-engineering attacks. Communications can now be highly personalised and professionally written.

### Why It Matters

Traditional signs of phishing, such as poor grammar and spelling mistakes, are becoming less common. Verification processes are now more important than spotting errors.

**Business Impact**
Credential theft; financial fraud; malware infections; business email compromise.

**Calder IT Recommendation**
Update awareness training to include AI-generated threats and verification procedures.

**Key Takeaway**
AI is making cybercrime more convincing, not fundamentally different.

## 4. Personal vs Business AI Accounts

### The Risk

Employees often use the same AI services at home and at work. Personal accounts typically exist outside organisational governance and security controls.

### Why It Matters

This creates uncertainty around data ownership, retention and compliance. Organisations may also lose visibility of how business information is being processed.

**Business Impact**
Loss of oversight; compliance concerns; inconsistent security; audit challenges.

**Calder IT Recommendation**
Business information should only be processed through approved organisational AI platforms.

**Key Takeaway**
Business information belongs in business systems.

## 5. Unapproved AI Integrations

### The Risk

Many AI products connect directly with Microsoft 365, email platforms, CRM systems and file storage services.

### Why It Matters

Poorly controlled integrations can expose sensitive information or grant excessive permissions. The greatest risk is often not the AI itself, but what it can access.

**Business Impact**
Data leakage; excessive permissions; third-party risks; security exposure.

**Calder IT Recommendation**
Apply the same governance and security reviews used for any business application.

**Key Takeaway**
Review what an AI tool can access before approving what it can do.

## 6. Shadow AI

### The Risk

Employees often adopt AI independently to improve productivity. While usually well intentioned, this creates governance, security and compliance concerns because the organisation lacks visibility.

### Why It Matters

Most shadow AI emerges when employees perceive a business need and no approved solution exists. This makes education and governance more effective than outright bans.

**Business Impact**
Lack of visibility; data protection concerns; inconsistent processes; security risks.

**Calder IT Recommendation**
Provide approved alternatives and practical guidance rather than attempting to prohibit AI completely.

**Key Takeaway**
You cannot govern technology you cannot see.

# AI Risk & Responsibility Guide

## Building Responsible AI Governance

Strong AI governance combines policy, technology, security and employee awareness. Organisations should treat AI like any other business technology with documented controls, accountability and oversight.

| Organisational area | What you can have in place |
|---|---|
| **Governance & Policy** | AI Acceptable Use Policy,<br>management ownership,<br>approval processes<br>risk reviews |
| **Security & Compliance** | Data protection guidance,<br>supplier due diligence,<br>security assessments<br>integration reviews |
| **People & Awareness** | Training<br>guidance on approved tools,<br>human review requirements<br>reporting processes |
| **Technology & Oversight** | Approved AI platforms,<br>integration reviews,<br>monitoring<br>auditing |

## How Calder IT Can Help

Whether you are evaluating Microsoft Copilot, reviewing existing AI usage, developing an AI Acceptable Use Policy, conducting security assessments or delivering staff awareness training, Calder IT can help your organisation implement AI safely, securely and responsibly.

**Key Takeaway:**
Organisations that gain the greatest value from AI are those that balance innovation with governance, security and accountability.