Outside Context
AI & DIGITAL TRANSFORMATION

BISG WEBINAR · 24 SEPTEMBER 2026

AI and risk in publishing

Building trust while managing change

George Walkley

Founder and Principal, Outside Context Ltd

INTRODUCTION

The Risk Landscape

amazon

Associated Press

BLOOMSBURY

CHICAGO SUN-TIMES

grammarly

hachette BOOK GROUP

HarperCollinsPublishers

The New York Times

Penguin Random House

Simon & Schuster

Every one of these organisations has experienced issues with AI, risk and trust in recent years

INTRODUCTION

My Perspective

- 30 years in bookselling and publishing, fifteen of them at Hachette in marketing, digital and strategy
- AI training, consulting and development with 400+ organisations in fifteen countries, working with the IPG, IBPA, and others
- Chair of Midas Group; non-executive director, Burleigh Dodds Science Publishing; advisory board, Bristol University Press
- Write a weekly newsletter on AI in media and publishing, new book *The Intelligence Multiplier* out in December

30
years in the trade

400+
organisations

15
countries

INTRODUCTION

Framing risk

- The question for this webinar isn't whether AI has a role in the books value chain, or the ethics of it
- It is pragmatic and practical: how we manage the technology and its risks—adopt, limit or opt out
- Inaction is its own form of risk: agency, competitiveness, cost and talent
- Four dimensions of risk
  - **Technology:** the models, platforms and terms you are building on
  - **Governance:** what the organisation permits, and what people actually do
  - **Content:** what goes into your workflows and out into the supply chain
  - **Relationships:** the trust of authors, colleagues, partners and readers
- Six proposed mitigations for each

Technology

- Pace of change: capability, features and whole products turn over in months, not traditional procurement cycles
- Volatility: cost, tiers, terms and access shift under you—often without notice
- Approval of one version of a model should not be a blank check for future generations—permissions need to be revisited with new models and/or significant change
- The enterprise default: most organisations inherit a model from their email and office suite (Copilot, Gemini).
  - **Upsides:** systems integration, SSO and admin controls
  - **Challenges:** functionality and capability lag, licence creep, and staff routing around it
- Integration raises switching costs: the deeper AI sits in your systems, the harder it is to leave

Governance

~1⁄3	3⁄4	1⁄3	17%
publishers with an AI policy, 2025	IPG members with a policy, 2026	workers using AI without their employer's knowledge	of AI users paying for tools personally
BISG/BookNet Canada; IPG	IPG/Oxford Brookes, Sept 2026	Deloitte, Sept 2026	Deloitte, Sept 2026

- Policy is not governance, but it is foundational—and the gap is closing fast
- In the absence of the right tools and frameworks, staff find their own way: many paying personally say the tool is better than the enterprise version
- Senior leaders twice as likely as junior staff to use “shadow AI” (BlackFog/Perplexity)
- The other direction: nearly 30% of workers admit to undermining their employer's AI strategy — refusing tools, ignoring policy, uploading documents to insecure models (Writer.com)

RISK 3 OF 4

Content

- Two aspects: undisclosed AI inputs to your workflows, and undisclosed AI outputs to your supply chain
- In-house: which stages already touch AI—editorial, translation, indexing, narration, metadata, marketing?
- Out-of-house: how do authors, illustrators, freelancers, indexers, translators, service providers, aggregators, retailers and readers use it?
- Is there clear disclosure, and a shared understanding of what represents AI use?
- Three debts:
  - **Technical:** the systems you need to maintain
  - **Strategic:** the options your choices close off
  - **Cognitive:** the judgement you no longer exercise

Relationships

- The books supply chain depends on trust—once lost, hard to regain
- Do partners know what they are getting, and does it change their perception of value?
- Signalling through metadata (C2PA, SynthID), certification, and disclosures: https://www.georgewalkley.com/how-i-use-ai/
- Not just a question of external partners—the “hot labor summer” (PW) and employee advocacy (New York Times, Hachette)
- Suspected AI use outside your guardrails raises questions about burden of proof and procedural fairness: the Authors Guild's test of five detectors found extreme variance, and it warns that pulling a book on a detector alone is a material breach of contract
- Author attitudes to AI are not monolithic and follow incentives: a third of academic researchers starting their research journeys with AI tools (Kudos); large majorities of UP authors opted in to AI licensing; trade authors are overwhelmingly reluctant (Creative PEC)

MITIGATION 1 OF 4

Technology

01 **Separate data from harness.** Keep content, metadata and workflows in systems you control; treat the model as a replaceable component.

02 **Build model-agnostic.** Prompts, skills and integrations that can move between models. Use MCP to connect models to data where it lives rather than uploading it.

03 **Do due diligence on vendors.** Where does the data go, is it retained, is it trained on, which tier do the terms apply to, and how do you leave? (IPG vendor framework)

04 **Measure usage before it becomes habit.** Who uses which tools, for what tasks, at what cost. Know your ROI so you know if the cost is proportionate (John Wiley)

05 **Question the default, don't just reject it.** If Copilot or Gemini is the platform, know what it can't do and where people will route around it. Identify your outliers.

06 **Experiment now.** Pricing is subsidised and access is generous; neither will necessarily last. Experimentation beats documentation.

MITIGATION 2 OF 4

Governance

01 **Write the policy.** Who owns it? Review it on a cadence, not on a crisis. Nature, OUP, Springer Nature, Wiley and CJR are usable templates.

02 **An approved-tools list and red lines.** E.g. unpublished manuscripts, author personal data, contracts and confidential material never go into consumer tools.

03 **Find out what is really happening.** Anonymous survey, usage data or an AI amnesty. Make disclosure safe, or you will only ever see the first case.

04 **Treat it as a data point, not a disciplinary matter.** A tool someone pays for personally is either a confirmed use case or a performance measurement problem. Either way, it is information about your policy and your tools.

05 **Don't set quantitative targets.** Amazon measured token consumption and got automation of pointless tasks. Goodhart's law: "When a measure becomes a target, it ceases to be a good measure."

06 **Protect the apprenticeship.** Experienced staff generally get the biggest productivity gains; reinvest that time in mentoring rather than pulling up the ladder.

MITIGATION 3 OF 4

Content

01 **Set disclosure norms before you need them.** What you ask of contributors, what you tell readers and partners, what you tell each other. (STM disclosure standard consultation closes 16 October)

02 **Sign off on explainability.** If nobody can explain why an output is right, it is not ready. AI does the research and analysis; people keep framing, deciding and accountability.

03 **Prefer declared provenance to detection.** Metadata disclosure, as Libby does, over detectors. Accept the occasional false negative rather than the false positive that ends a career.

04 **Never rely on a detector alone.** Software and watermarks prove text was processed, not who wrote it. Disclose your methodology and give authors a fair hearing.

05 **Use AI to check as well as to create.** Fact-checking agents are coming for backlists whether publishers run them or not. Better to run them yourself.

06 **Calibrate the response to the case.** Deceptive, careless and blown out of proportion are three different problems and need three different answers.

MITIGATION 4 OF 4

Relationships

01 **Tell partners how you use AI on their work.** In contracts, guidelines and conversation. Disclosure should be reciprocal and upfront, not one-way and retrospective.

02 **Ask partners how they use it.** Authors, freelancers, service providers, platforms. Write the question into briefs, statements of work and contracts.

03 **Review contracts for the platform layer.** AI is becoming a standard feature for many retailers, both behind the scenes and in reading experience. A 'no AI' clause may have unintended consequences.

04 **Run the fire drill.** A cloned author voice, a detector accusation, a retailer pulling a title: who takes the call, what do you say, who decides?

05 **Put procedural fairness in writing.** A process for suspected undisclosed AI use, with a burden of proof and a right of reply, before you need it.

06 **Own mistakes publicly.** Almost everyone will have their moment.

THANK YOU

Questions

Context Window

A weekly newsletter on AI in media and publishing, trusted by 2,500+ readers
Subscribe at www.georgewalkley.com/newsletter

The Intelligence Multiplier—published December 2026

Print and ebook: Practical Inspiration Publishing, Two Rivers
Audiobook: Penguin Random House Audio
Preorder at www.georgewalkley.com/books/the-intelligence-multiplier

linkedin.com/in/georgewalkley

hello@outsidecontext.co.uk