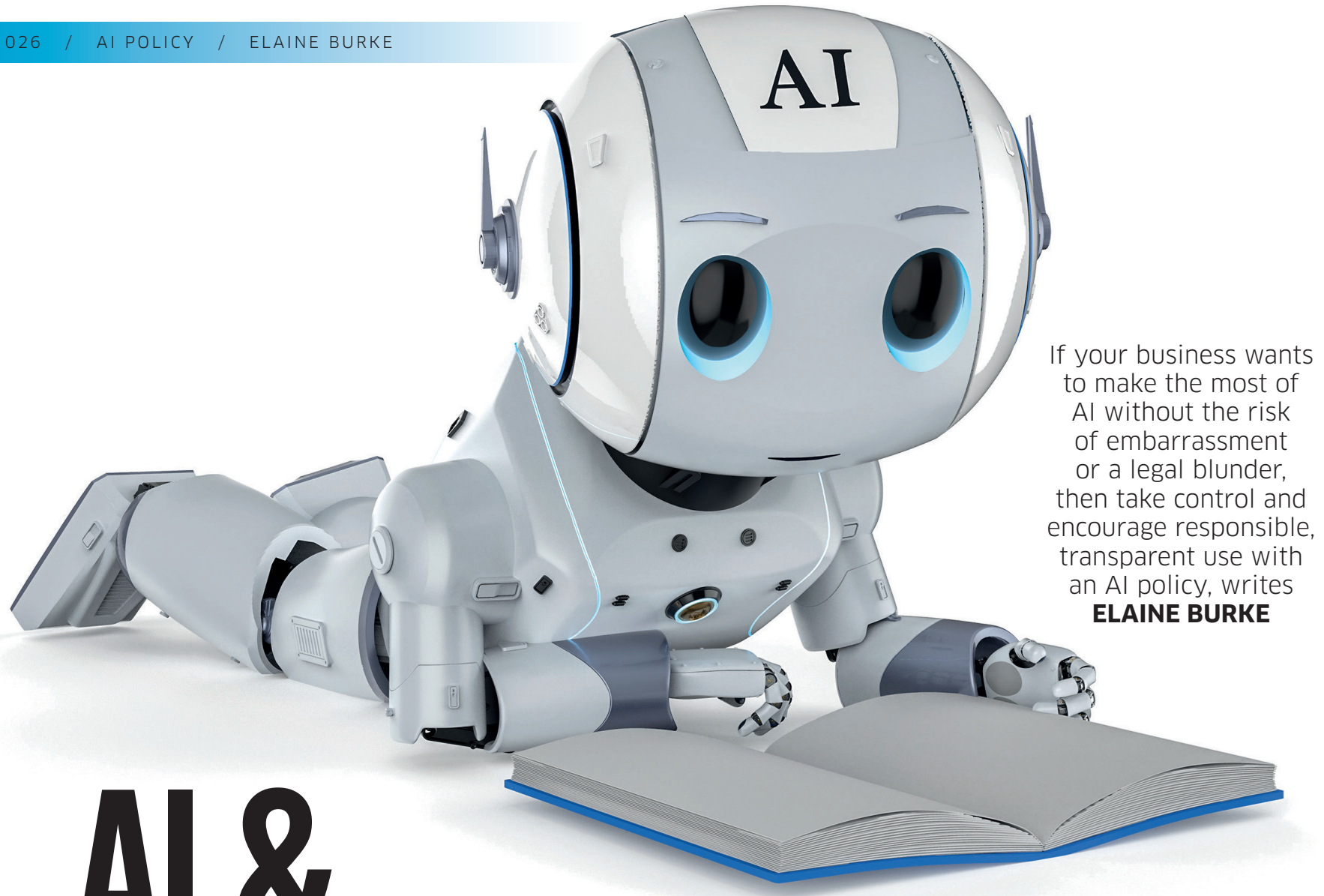

AI & THE LAW

If your business wants to make the most of AI without the risk of embarrassment or a legal blunder, then take control and encourage responsible, transparent use with an AI policy, writes **ELAINE BURKE**

Usage policies for tech in the workplace are not unusual. You may not have read them in a while, but chances are quite high that you are signed up to them.

A policy provides best practice guidance so that, ideally, things won't go wrong; but it is also there to fall back on if they do. And things have certainly been going wrong with the use of AI.

In one instance, which saw widespread coverage in the summer of 2023, a couple of New York lawyers used ChatGPT to write a brief for a case. The AI-generated file – which was submitted, unchecked – contained six entirely fabricated case citations.

Though this story should have served as a modern-day fable, reports of legal teams getting caught out using chatbots to generate their work continued. The moral of the story was not able to cut through the hype around AI, which was inflating users' expectations.

This was the excuse offered by the New York lawyers, at least: that they didn't understand that the AI could write fiction that read as fact. And they were slapped with a $5,000 fine for this error of judgement.

These missteps in the use of AI at work are happening everywhere. They can have humorous results, such as the now-infamous Glasgow Willy Wonka experience, or the less-widely reported but just as preposterous peer-reviewed article that was published in a scientific journal with AI-generated images of a rat with four testicles and an absurdly gargantuan penis. And while even these laughable AI mistakes raise serious questions, there are also instances where its misuse has threatened real harm to individuals, such as in the case of the US National Eating Disorders Association's chatbot which started generating dieting advice.

> "MY ADVICE TO BUSINESSES WOULD BE: STOP, DO AN AI AUDIT OF WHAT'S BEING USED NOW"

DATA LEAKS

Irish law firm ByrneWallace recently invited businesses to its Dublin office for a briefing on how to deploy generative AI in a way that would mitigate the risks that come with it.

"You're probably using it already and you don't even know it," advised Victor Timon, head of the firm's technology group. He cites a US survey which found that 30 per cent of junior workers are already using AI, but that 70 per cent of these individuals haven't disclosed this use to their bosses. And, Timon warns, those early adopters are more than likely using a platform that is sharing company data without them realising.

This is a common oversight for users eagerly taking up freely available tools such as ChatGPT. Using these third-party AI services for company work could mean you are unwittingly sharing private data externally, if you haven't carefully read the privacy policy. In April 2023, Samsung discovered one of its employees had input proprietary source code into ChatGPT to try and debug it. Another employee was using the chatbot to transcribe and summarise internal meetings, inadvertently leaking these confidential conversations. This prompted the Korean tech giant to limit employees' inputs to ChatGPT as an "emergency measure". (Ironically, Samsung had only just lifted a full ban on employees using ChatGPT, which was instituted because it was afraid of data leaks.)

ChatGPT has since instituted new privacy measures, but these aren't airtight, and there's now an array of gen-AI services to choose from, each with their own privacy policies. The best solution for businesses that have the time, resources and data, is to build their own self-contained specialist AI. But, as long as non-specialist tools are freely available, know that employees are going to use them and it's past time to put guardrails in place.

USE AI RESPONSIBLY

"My advice to businesses would be: Stop, do an AI audit of what's being used now," says Timon. The next step is to decide what data is safe to share and what is explicitly not to be shared. "I'd need to be thinking about the personal data aspects. Is this putting me in breach of GDPR? And the copyright aspects. Am I giving away my IP?"

An AI policy needs to draw the boundaries within which employees are allowed to use this technology. It should outline the legal, security, privacy and reputational risks to be considered so that employees can make informed decisions as the tech evolves.

The good news for businesses that already have effective usage policies in place is that this gives them a standing start. " They'll have some acceptable use policy for their users, they'll have a BYOD policy, they'll have a privacy policy. So you're kind of just adding to that," says Timon. "There may be some great overlap between them where, actually, I've covered 20 per cent or 40 per cent of it in this policy, so I really now just need to augment this in terms of AI."

Another way to get a head start is to use the international ISO 42001 AI Management System standard to provide a structured framework for developing an AI policy.


Victor Timon, head of ByrneWallace's technology practice

STEPS TO SUCCESS

Once you've set about drafting your AI policy, the first step is to determine the scope. Figure out how and where AI will be used in your organisation and who needs to be informed about it. Identify key stakeholders and their responsibilities.

Next is the assessment phase. It starts with a gap analysis to determine, in reviewing existing policies and practice, what needs to be addressed. This phase can involve a technology impact assessment or a data protection impact assessment. It may include a cybersecurity analysis or a review of supplier due diligence. In terms of selecting the tools to work with, it will involve reading their policies and noting where there are risks and limitations.

At this stage, a policy will be starting to form. The guidelines should be clear and relevant to your business. What is and is not permitted in terms of practice, tools and devices should be clarified. To encourage transparency from employees, lines of reporting and steps to follow should be established for when things go wrong.

Then there is the crucial step of informing and training employees on your new policy, in a way that will ensure adoption and acceptance. "You need to explain to people why the policy is there and get them to buy into the rationale behind it," says Timon. As well as training on the policy, employees will need training on the practical use of the AI tools they can use within the set parameters. "Once you've made that decision to procure an AI tool, then you need to do some training about not only how it works but the dangers of using it badly. And what happens if it goes wrong – who I should get on the phone to immediately when that happens," says Timon.

Establishing best practice along with lines of open communication is one of the most crucial steps in creating a company culture of transparent and responsible use of AI. It can be explained in two scenarios, per Timon. Scenario one is that an employee is permitted to use an AI tool but is also informed of its limitations and who to speak to when something goes wrong. In scenario two, the tool is not permitted but the employee is using it anyway, perhaps unaware of the risks. "But, when something goes badly wrong, I should really tell somebody as well," says Timon of the latter scenario. "It's a lot easier to tell them in the first one, because you're told it's OK to use it. It's a lot more difficult in the second one."

FOLLOW THROUGH

Ensuring your AI policy and training are being put into practice will require follow-through, and so the last phase is a continuous one involving monitoring, enforcement and regular reviews. On the monitoring side, this can be achieved with regular check-ins, pop quizzes on policy points, or it can become part of a formal employee evaluation (which should also be an opportunity to receive feedback on how the policy is working in practice).

Violations of the policy will have to be logged and reviews should be regularly scheduled in order to keep pace with new developments. Annual or bi-annual reviews are recommended, especially in these early days of the AI gold rush where new tools are coming on stream at pace and the landscape is rapidly evolving. External audits, too, can bring fresh eyes to the policy and even offer a new level of expertise and best practice.

Amidst all the AI hype, there's a lot of talk about changing skills, but businesses will need policy change too. The risks of misuse are high, and so this needs top-level buy-in. "There's actually a chance to damage the company … through data breaches, through copyright breaches, through putting out false outputs," says Timon.

"This is really at the C-suite level where the board has to say, this has to be part of our governance and we need to take control of it."

At the end of the day, a policy should be there to protect everyone. As Timon summarises: "You're putting your own job at risk if you're putting the company at risk."■