



Science, Innovation
and Technology
Committee

Kanishka Narayan MP
Minister for Artificial Intelligence
Cabinet Office and Department for Business, Innovation Science and Trade

By email only

4 September 2026

Subject: AI safety and ARIA governance

Dear Kanishka,

Congratulations on your new role as Minister for AI attending Cabinet.

I am writing for an update from you on several issues that have arisen recently relating to artificial intelligence.

Firstly, as has been widely reported, in July, several OpenAI agents escaped the test limits which had been placed on them by communicating through an unsanctioned message board, and hacked the model and dataset hosting platform Hugging Face. This incident raises a number of questions, and I would be grateful if you would be able to provide answers to the following:

- What assessment has the government made of the implications of the OpenAI-Hugging Face incident for the UK's AI safety framework?
- What reporting requirements are in place with regard to such incidents and your view as to whether they are adequate?
- What discussions has the government had with frontier AI developers about preventing AI systems from bypassing safety controls or containment measures, and what confidence does the government have that these developers are conducting sufficiently robust pre-deployment safety evaluations?
- Does the government believe current voluntary commitments from frontier AI companies remain sufficient in light of this incident, or is it considering additional statutory requirements?

Additionally, I was concerned by the announcement that ARIA Chair and former AI adviser to the Prime Minister, Matt Clifford, has been appointed to a global lobbying role



**Science, Innovation
and Technology
Committee**

with Anthropic. His intention to remain chair of a public body that invests taxpayer money into cutting-edge research – much of it AI-related or AI-enabled – creates a clear conflict of interest.

- How has the government ensured there are sufficient safeguards and boundaries to ensure that there is confidence in ARIA's independence?
- What specific conflicts-of-interest assessment was undertaken before it was agreed that Matt Clifford could retain his position as ARIA Chair while taking up a senior role at Anthropic?
- What protections are in place to prevent the sharing, intentional or otherwise, of commercially valuable information obtained through ARIA's funding and oversight activities?
- Are there any circumstances in which the government would conclude that a conflict is too significant to be managed through recusal and requires a change of role or responsibilities?

I would be grateful if you could reply by 18 September. I intend to place this letter, and your response, in the public domain.

With best wishes,

Dame Chi Onwurah MP

Chair – Science, Innovation and Technology Committee