Reference: 2026-031

Thank you for your email in which you requested the following information under the Freedom of Information Act 2000 (FOIA):

I am requesting information relating to personal data incidents and GDPR breaches that have occurred as a result of the use of artificial intelligence (AI) tools within your organisation. The time period covered by this request is 1 January 2022 up to and including the date on which this request is processed by your organisation. When referring to confidential or sensitive government information I am referring to any documentation or information placed into an AI Chatbot that was not intended or not cleared for publication. For the purposes of this request, this includes incidents arising from or connected to:

- **AI chatbots (including but not limited to ChatGPT, Google Gemini, Microsoft Copilot, or any equivalent large language model tool).**
- **AI tools that were not formally authorised or approved for use by your department or organisation.**
- **AI tools used in an unauthorised manner — that is, tools which may have been approved in principle but were used outside their permitted scope, purpose, or in contravention of departmental policy.**
- **AI tools designed to summarise, transcribe, or record meetings or communications (including, for example, Otter.ai, Fireflies.ai, Microsoft Copilot meeting summaries, or equivalent tools).**
- **Any other AI system or tool through which personal data or special category data was entered, processed, shared, or transmitted without appropriate authorisation or adequate data protection safeguards.**

Information Requested:
For each personal data incident of GDPR breach falling within the scope set out above, please provide the following:

1. Nature of the Data Involved

a. **Whether the data was personal data or special category data (as defined under the UK GDPR and the Data Protection Act 2018).**
b. **A general description of the category or type of data involved (for example: names, contact details, health or medical information, financial data, immigration status, criminal records, etc.**

2. Number of Individuals Affected

a. **The number of data subjects whose personal data was involved in or affected by the incident.**

3. Date and Time of the Incident

a. **The date and time at which the incident occurred, or — where the exact time is not recorded the approximate date.**

4. Reporting to the Information Commissioner's Office (ICO)

a. **Whether the incident was reported to the Information Commissioner's Office (ICO).**
b. **Where applicable, the date and time the incident was reported to the ICO.**

5. Outcome and Remedies

The outcome of any internal investigation into the incident:

a. **Any remedial, corrective, or preventive action taken by your organisation as a result.**
b. **A copy of any documentation recording the outcome or remedies applied, including any written decisions, reports, or correspondence with the ICO arising from the breach**

6. Notification of Affected Individuals

a. **Whether the individuals directly affected by the breach were informed of the incident.**
b. **If so, the date on which notification was provided to them.**

Confidential and Sensitive Information

In addition to the personal data incidents described above, I also request information on the broader use of AI tools in circumstances where confidential or sensitive government information was entered into or processed by such tools, regardless of whether this constituted a formally recorded personal data breach. When referring to confidential or sensitive government information I am referring to any documentation or information not intended or not cleared for publication.

Specifically, please provide:

7. Number of Recorded Incidents

a. **The total number of occasions on which confidential or sensitive government information was entered into, uploaded to, or otherwise processed by an AI tool during the period 1 January 2022 to the date of processing.**
b. **A breakdown of these incidents by year, where this information is held.**

8. Classification or Sensitivity of Information Involved

a. **Whether any of the information involved was classified under the Government Security Classifications (GSC) policy (i.e. OFFICIAL, OFFICIAL-SENSITIVE, SECRET, or TOP SECRET).**
b. **The number of incidents involving each classification level, where recorded.**
c. **Whether any incidents involved information subject to legal professional privilege, commercially sensitive data, or information relating to national security.**

9. Type of AI Tool

a. **Whether the AI tool used was an externally hosted or third-party tool (i.e. not hosted**
   on government or departmental infrastructure).
b. **Whether the AI tool was authorised for use by the department at the time of the incident.**
c. **The name or category of AI tool involved, where this information is held and can be disclosed.**

10. Policy and Guidance

a. **Whether your organisation had a policy or guidance in place governing the use of AI tool in relation to confidential or sensitive information at the time the incidents occurred.**
b. **If so, the date from which such a policy was in place.**

c. **Whether any policy or guidance has been updated or introduced as a direct result of incidents of this nature.**

11. Outcome and Action Taken

a. **Whether any formal investigation, disciplinary action, or security review was carried out as a result of any such incident.**
b. **A summary of the outcomes or actions taken, in aggregate where individual details cannot be disclosed.**

Response

We are writing to advise you that following a search of our paper and electronic records, we have established that the information you requested is not held by the SFO.