

The AI Narrative Index

How the Machines See Your Brand

Generative AI is the new search engine. When investors, journalists, and customers ask ChatGPT, Gemini, or Perplexity about your industry, does your brand appear as a market leader — or is it defined by past crises and low-quality sources? This report measures your AI narrative across four scored pillars and one independent safety check.

ChatGPT Google Gemini Perplexity

SCORING ENGINE

$AI\ Score = (V \times 0.35) + (R \times 0.25) + (F \times 0.20) + (C \times 0.10)$

V
35%

VISIBILITY — THE LEADERSHIP TEST

Does the AI naturally recommend you as a Top 5 leader in your industry? We ask each AI to rank the market. #1 rankings score maximum points; complete invisibility scores zero.

e.g. "Who are the top banks in Singapore?" — If DBS is ranked #1, full points. If a competitor is missing entirely, they score zero.

R
25%

REPUTATION — THE RISK TEST

Is your AI footprint weighed down by past crises? We scan the AI's memory for historical fines, scandals, and controversies. Each confirmed event subtracts from a perfect 100.

e.g. A 2019 regulatory fine may still appear as the #1 fact the AI associates with your brand — years after resolution.

F
20%

SOURCES — THE AUTHORITY TEST

Who is the AI listening to? We extract the URLs the AI cites. Tier 1 sources (Bloomberg, government sites) score high; unverified blogs and forums score low.

e.g. If 60% of your citations come from Reddit threads instead of Reuters, the AI is building your narrative on unreliable ground.

C
10%

CONSISTENCY — THE ALIGNMENT TEST

Do different AI models agree on your corporate story? We cross-check ChatGPT, Gemini, and Perplexity. Factual contradictions trigger penalties.

e.g. Gemini says your CEO is "John Smith" while ChatGPT names someone who left in 2019 — that confusion reaches users daily.

INDEPENDENT SAFETY CHECK

T
INDEPENDENT

TRUTHFULNESS — BRAND SAFETY GUARDRAIL

Even if your VRFC score is high, AI can invent facts. We deploy an auditor to fact-check the models against real-world data — catching fabricated executives, invented acquisitions, or competitors' achievements attributed to your brand. Tracked independently.

e.g. ChatGPT claims your company "acquired XYZ Corp in 2023" — an event that never happened. This could mislead investors and analysts.

ASSESSMENT PIPELINE

1

Interrogation

AI platforms queried with proprietary prompts

2

Fact-Checking

Responses audited against real-world data

3

Strategic Output

Scores calculated and action plan generated

Royal Mail: AI Brand Health Report

Industrials | Generative AI Narrative Assessment

AI BRAND HEALTH CLASSIFICATION

Vulnerable

AI narrative has significant gaps

OVERALL SCORE

62.6

out of 100

VISIBILITY (V) 100.0 Healthy	REPUTATION (R) 16.0 Critical	SOURCES (F) 58.9 At Risk	CONSISTENCY (C) 60.0 At Risk	TRUTHFULNESS (T) 80.0 Healthy
--	--	--	--	---

Executive Summary

Royal Mail dominates AI visibility across major platforms, consistently ranking #1, but its overall AI Brand Health Score of 62.6 is classified as "Vulnerable" because high discoverability is amplifying a crisis-heavy narrative. The biggest strength is category leadership presence in AI answers, while the biggest vulnerability is a severely exposed reputation footprint driven by repeated Ofcom fines and service reliability concerns that AI surfaces as core brand descriptors.

AI Platform Visibility

OPENAI

#1

Industry Rank

GEMINI

#1

Industry Rank

PERPLEXITY

#1

Industry Rank

Narrative & Brand Safety Assessment

Reputation (R: 16.0) & Consistency (C: 60.0) Analysis

REPUTATION SCORE

16.0

8 crisis events detected

CONSISTENCY SCORE

60.0

2 discrepancies

TRUTHFULNESS SCORE

80.0

3 platforms verified

Crisis Events Detected by AI Models

SEVERITY	EVENT	SOURCES
Formal Penalty	Royal Mail was fined for three consecutive years by Ofcom for failing to meet statutory delivery targets. In 2022/23, it was fined £5.6M....	openai, gemini, perplexity
Confirmed Systemic	In June 2026, Ofcom opened a new investigation into Royal Mail's 2025/26 delivery performance after the company again missed annual targe...	openai, gemini
Confirmed Isolated	In March 2025, a hacker leaked 144GB of data (approx. 16,000 files) allegedly stolen via third-party supplier Spectos. The leak included ...	gemini
Confirmed Systemic	In January 2023, the LockBit ransomware group targeted Royal Mail, forcing a total halt to international shipping services for three week...	gemini
Confirmed Isolated	A technical glitch in November 2022 allowed customers to see order histories and personal details of other users, leading to a temporary ...	gemini
Confirmed Systemic	Over 115,000 workers participated in 18 days of industrial action between 2022 and 2023, causing massive backlogs and contributing to a £...	gemini, perplexity

+2 more events

Truthfulness Verification by Platform

OPENAI

4/5

GEMINI

5/5

PERPLEXITY

3/5

Cross-Model Discrepancies

- Gemini and Perplexity provide contradictory rankings for the second-largest parcel carrier in the UK; Gemini identifies Evri as the largest dedicated domestic network following a 2025 merger with DHL, while Perplexity ranks Amazon Logistics as the second-largest player by market share.
- Gemini claims Royal Mail was acquired by the Czech-based EP Group in early 2025, whereas other platforms describe it as currently operating under International Distribution Services (IDS) plc without confirming a completed acquisition.

Narrative Assessment

Reputation is critically compromised (R: 16) with AI repeatedly foregrounding three consecutive years of Ofcom penalties, including a £21M fine tied to only 77% First Class delivery versus a 93% target, plus a fresh Ofcom investigation opened in June 2026. Data privacy incidents also appear, including the January 2023 LockBit ransomware disruption of international shipping and the March 2025 third-party leak allegation involving 144GB of data, creating a compound reliability and trust risk. Truthfulness is comparatively strong (T: 80), but Perplexity underperforms (3/5) and models surface unverified lawsuits (£900M class action claim, £600M Whistl claim) that can influence investor and procurement perceptions even when not substantiated. The corporate risk is that customers, regulators, and capital markets receive a simplified AI narrative: systemic performance failure plus cyber vulnerability, which can harden into assumed fact without proactive narrative correction.

Media Authority & Ecosystem

Visibility (V: 100.0) & Sources (F: 58.9) Analysis

VISIBILITY SCORE

100.0

AI platform detection rate

SOURCES SCORE

58.9

48 unique sources cited

TIER 1 SOURCES

10

Gov / Top Press citations

Source Tier Distribution

- Tier 1 (Gov/Press): 10 (21%)
- Tier 2 (Quality Media): 7 (15%)
- Tier 3 (Industry/Corp): 21 (44%)
- Tier 4 (Blogs/Forums): 10 (21%)

Top Cited Domains

DOMAIN	TIER
ofcom.org.uk	Tier 1
gov.scot	Tier 1
news.sky.com	Tier 1
hansard.parliament.uk	Tier 1
publications.parliament.uk	Tier 1
committees.parliament.uk	Tier 1
theguardian.com	Tier 1
bbc.com	Tier 1
tandfonline.com	Tier 1
independent.co.uk	Tier 1

Authority Gap Analysis

Visibility is maximal (V: 100), so Royal Mail is being treated as the default category reference point, but the supporting evidence base is mid-quality (F: 58.9) with meaningful reliance on Tier 3 and Tier 4 sources (31 of 48), increasing the odds that outdated or speculative claims persist. While Tier 1 citations exist (Ofcom, Parliamentary sources, top press), they are not sufficiently crowding out lower-authority sites, allowing mixed-quality context to shape AI summaries. Cross-model inconsistency also creates governance risk: Gemini suggests an EP Group acquisition in early 2025 while other platforms still frame Royal Mail under IDS without confirmation, and models disagree on competitor scale and rankings. In practice, Royal Mail is winning attention but not controlling the evidentiary spine of the story, which is why leadership visibility is not translating into brand safety.

Strategic Agency Recommendations

Actionable PR & Communications interventions for Royal Mail

6-Month Action Plan

Based on the audit findings, the following interventions are recommended to improve Royal Mail's AI brand health scores. Each recommendation is tied directly to a weakness identified in the data.

Recommendations

- 1

Regulatory performance narrative reset
Create a Tier 1 anchored communications package that reframes Ofcom outcomes around a clear improvement roadmap, with audited KPIs, milestones, and customer impact metrics, then place it through top press and policy channels that AIs already cite (Ofcom-adjacent coverage, Parliamentary correspondents, business desks). Build an always-on "service performance" newsroom page that updates monthly and is optimized for AI retrieval so the next answer leads with progress, not penalties.
- 2

AI source-quality uplift and owned-asset hardening
Audit the top AI-cited URLs and publish authoritative replacements on royalmail.com and Wikipedia-compatible sources, prioritizing pages that address delivery targets, governance, and cyber resilience, then interlink them to concentrate authority and reduce Tier 4 reliance. Add structured data (Organization, FAQ, NewsArticle) and a controlled "facts and timeline" section to reduce hallucination and dampen repetition of unverified lawsuit claims.
- 3

Cyber trust and third-party risk comms program
Launch a cyber trust narrative that explicitly distinguishes confirmed events (LockBit 2023 disruption) from alleged supplier-related leaks, and document controls, supplier assurance, and incident response upgrades in a way journalists and analysts can cite. Secure Tier 1 validation through credible third parties (independent assessments, security standards, insurer or auditor commentary) to shift AI summaries from breach headlines to resilience proof points.

CURRENT SCORE SNAPSHOT

62.6	100.0	16.0	58.9	60.0	80.0
Overall	V	R	F	C	T (Independent)