

Is bristolpost.co.uk safe? TrustSniffer's moderate-trust assessment: 70/100

bristolpost.co.uk

Verdict

70

OUT OF 100

MODERATE TRUST

bristolpost.co.uk is moderately trusted.

Most signals looked ordinary, and some evidence was missing. Read the checks below before you pay or hand over personal details.

Safe for Read-Only

Assessed 2026-08-17 by automated analysis. Classification confidence 55%.

What this site appears to be

Regional news homepage (Bristol Live) with headlines across news, sport, events and lifestyle. Cookie/privacy consent and a paid option to remove ads are present. Content appears editorial and informational.

Evidence status and limitations

Evidence completeness: UNKNOWN

- The real-world operator identity was not independently verified.
- Module-level completeness metadata is unavailable for this legacy report.

At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	Not available No registration record was returned	NOTED
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by Amazon RSA 2048 M01	NOTED

The page as captured

<https://www.bristolpost.co.uk/>



What bristolpost.co.uk served when TrustSniffer captured it on 2026-08-17. The page may look different now.

Key findings

- Automated classification: Safe for Read-Only.
- No flags from the reputation services TrustSniffer consulted at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Overview

This website presents as Bristol Live, a regional news publisher covering Bristol-area news, sport, business, events, traffic, crime, and entertainment. Its apparent business model is ad-supported editorial publishing, supplemented by an optional Privacy Plus subscription that removes advertising and reduces advertising-related data sharing.

Scam/Impersonation Risk

No phishing, impersonation, blacklist, or other contradictory signals were observed. The homepage is editorial and informational, with no login form, sensitive data form, wallet connection, or apparent credential-harvesting mechanism. Some interaction telemetry recorded external network activity as suspicious, but the associated assessment found no cloaking, hidden forms, password exfiltration, wallet-drainer behavior, clipboard hijacking, or suspicious inline scripts; this is therefore not evidence of impersonation. A clean set of evaluated threat-reputation checks further supports the absence of an active malicious signal.

EVIDENCE

- Homepage: regional news content was present, with no login form or sensitive form identified.
- Interaction behavior: no cloaking, hidden forms, password-external forms, wallet-provider activity, wallet-drainer runs, or clipboard writes were detected.
- External reputation checks: 0 malicious and 0 suspicious detections were recorded; the site was evaluated across the available coverage.

Regulatory Verification Notes

The available content is consistent with an established local-news publishing model rather than a financial or investment service. The site's real-world operator identity is not independently verified, and its on-page legal and governance disclosure is unclear; this limits attribution without creating a contradiction or demonstrating fraudulent intent. No financial license claim or license number is presented in the supplied content, which is a transparency item to resolve only if the proposed engagement involves regulated or payment-related activity. The site nevertheless has a meaningful global traffic footprint, mid-range page authority, clean evaluated reputation, and technically valid transport security, providing convergent support for an apparently legitimate operating website.

EVIDENCE

- Homepage: the stated model is advertising-supported local journalism with an optional paid ad-removal service.
- Hosting telemetry: served from AS16509, AMAZON-02 - Amazon.com, Inc., US.
- Transport security: TLS certificate issued by Amazon RSA 2048 M01, validation level DV, valid to 2027-01-02T23:59:59+00:00.
- External presence: traffic rank 18531 and mid-band page authority were recorded; no malicious or suspicious reputation detections were recorded.

What to Verify Next

Before sensitive or high-value interaction, independently confirm the legal operator and the official contact channels using a separately sourced route. The Terms and Conditions should be reviewed for subscription renewal, cancellation, refund, and payment provisions, while the privacy settings should be checked to confirm the intended consent and data-processing choices. If any activity extends beyond ordinary news access, the relevant licensing or registration position should be confirmed with the applicable official registry.

EVIDENCE

- Terms and Conditions: identified by the homepage as the governing document for the paid service.
- Privacy controls: the homepage provides consent-management and preference options for advertising-related processing.
- Independent verification: the available evidence does not independently connect the website to a verified real-world operator.

Summary Verdict

The website has a **moderate-trust posture** and is consistent with a functioning, established informational publisher, with no observed scam or impersonation contradiction. Its legitimacy is apparent from the convergence of substantive editorial content, established audience signals, clean reputation checks, and stable technical operation, but the operator identity remains unverified.

Infrastructure Integrity

The website is protected by AWS CDN/WAF infrastructure, with observed addresses belonging to CDN edge servers and no origin-server address exposed in the observed resolution. This reduces direct origin exposure and is a mitigating infrastructure characteristic, but it does not independently prove the identity or legitimacy of the operator.

Closing Assessment

Routine informational browsing is proportionate; sensitive submissions, paid commitments, or other high-value actions should follow independent confirmation of the service identity, applicable terms, and payment protections.

Written analysis generated 2026-08-17 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

No rule findings contributed to this verdict.

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	50%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of bristolpost.co.uk.

- The request stayed on bristolpost.co.uk. It was not redirected to another domain. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	Not available
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	13.33.235.94
Name servers	Not available

SSL issuer	Amazon RSA 2048 M01
SSL expiry	2027-01-02
Domain age	Not available (no registration date was returned)
Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about bristolpost.co.uk at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/bristolpost.co.uk> · assessed 2026-08-17