

UK Good Practice Principles certificate



Company: Nano Interactive
 15 Rathbone Place, 4th & 5th Floors
 Fitzrovia, London
 W1T 1HU
<https://www.nanointeractive.com/>

Business/Brands verified:	Nano Interactive
Service provided:	Platform, Technology
Month of verification:	November 2018

Findings

Good Practice Principles	Description of compliance with the Principles
<p>1 Educate yourself about traffic fraud and the risks that it poses to your business</p>	<p>Nano Interactive employees are encouraged to keep up to date with ad fraud developments by subscribing to key industry newsletters from sources such as Meetrics and IAS (Integral Ad Science).</p> <p>Employees also attend industry events such dmexco, Internet World and d3con.</p> <p>Nano Interactive have monthly meetings which are the basis of training and discussion including information sharing.</p> <p>All employee training is internal and information/reports are shared via an internal system.</p> <p>Senior staff are regularly involved in sharing information industry-wide through various news channels.</p>
<p>2 Adopt policies and strategies to identify fraud and mitigate its impact</p>	<p>The majority of campaigns are run through two DSPs, both of which audit inventory using both manual and automated processes. Nano has agreements with the DSPs to carry out this service and has reviewed the DSP policies to audit inventory. The DSP's filter data for ad fraud and report back to Nano Interactive on each campaign on anomalies such as invalid impressions or invalid clicks.</p>

Good Practice Principles	Description of compliance with the Principles
	<p>Nano also do their own checks on sites, manually checking for suspicious traffic, and high click through rates (CTR). Each campaign is monitored by the Ad Ops team at Nano Interactive on a daily basis. If the CTR is too high, or if suspicious activity is identified Nano Interactive contact the DSP to discuss. If potential ad fraud is confirmed the site is added to the blacklist to prevent serving inventory on that domain again.</p> <p>Nano Interactive have a detailed blacklist procedure.</p> <p>Nano Interactive’s Brand Safety Policy also details ad fraud processes such as vetting, 3rd party content verification, blacklists and whitelists and is located publicly on their website at: http://www.nanointeractive.com/brand-safety</p> <p>Integral Ad Science (IAS) can also, on client request, be used post-bid to verify fraud metrics to validate and monitor Nano Interactives internal detection tools.</p> <p>All tools referred to above, and in the sections below, are non-JICWEBS certified and not tested by ABC.</p>
<p>3 Set clear objectives for your media campaigns that focus on the measurement of real ROI, which is difficult for fraudsters to falsify.</p>	<p>Campaign objectives are client led and based on the client’s communications objective as discussed with the client via phone and email. Campaign objectives are set through Insertions Orders (IO’s).</p> <p>Objectives vary by clients but are mostly CPM (Cost per Mille), although CPA (Cost per action) and CTR (Click through rate) can be used if required.</p> <p>If CTR is used this is a KPI fixed for the advertiser, fluctuations are monitored and the KPI is benchmarked against acceptable levels.</p> <p>The client receives weekly reporting on their campaign and once the campaign is complete a Nano Account Manager creates a Post Campaign Analysis (PCA) report detailing campaign delivery details and trends.</p> <p>Nano Interactive measure campaign performance using their internal data, but also track using third party reports.</p>
<p>4 Practice safe sourcing and trust only business partners who have earned trust</p>	<p>Nano Interactive use inventory from two DSPs and a few vetted publishers. Nano has agreements with the DSPs to filter and audit inventory and has reviewed the DSP policies to do this.</p> <p>For the publishers partnered with directly, Nano Interactive has a vetting process, including a checklist of multiple verification steps that need to be completed before accepting a new publisher. Steps include: size of the publisher, available slots to monetise, search terms, position on the market, type of incoming traffic, privacy check, website check, technology in use, type of integration, trackers on the website, Ads.txt and CMP status.</p>

Good Practice Principles	Description of compliance with the Principles
	Nano Interactive regularly check for anomalies and raise any queries with the DSP as mentioned in GPP 2 and work with well-established partners and networks only.
<p>5 Implement technology to detect and prevent fraud</p>	It is the partner DSPs that use technology to filter data for ad fraud and report back on the campaign level as invalid impressions or clicks. When Nano Interactive deal direct with publishers they use Integral Ad Science tools to monitor invalid traffic including: high click-through rates, invalid impressions and ad-fraud percentages per domain.
<p>6 Filter traffic through vendors who prioritise fraud detection</p>	Nano Interactive vet all publishers prior to partnering with them (GPP4), DSP's use their own ad fraud detection tools, and Nano Interactive use Integral Ad Science tools along with their own internal checks on all campaigns (GPP5).

Verified by

Company: ABC Ltd
 Saxon House,
 211 High Street,
 Berkhamsted,
 Hertfordshire.
 HP4 1AD



<p>Statement of verification provider:</p>	<p>We have reviewed Nano Interactive’s policies and procedures for reducing risk to exposure to ad fraud in accordance with the JICWEBS Good Practice Principles. Our enquiries were designed to independently confirm that the anti-fraud policies stated have been implemented and clearly documented where required. Our review did not extend to testing the effectiveness of any processes, procedures or controls for ad fraud. In our opinion, at the time of our review, Nano Interactive had established policies to minimise the risk of ad fraud as described in the JICWEBS Good Practice Principles.</p>
--	---

About JICWEBS

JICWEBS (The Joint Industry Committee for Web Standards in the UK and Ireland) was created by the UK and Ireland media industry to ensure independent development of standards for measuring performance online and benchmarking best practice for online ad trading.

About the JICWEBS Anti-Ad Fraud Commercial Group

The Anti-Ad Fraud Commercial Group is an industry body made up of representatives from across the digital display advertising ecosystem, including the buy- and sell-side. It comprises representatives from advertisers, agencies, agency trading desks, demand side platforms, advertising exchanges, sales houses, advertising networks, supply side platforms and publishers.