The Content Verification Guide
The internet has revolutionised the way businesses work, how consumers spend their time, how stories and the news is told, read and shared. The digital revolution has led to the emergence of a multi-billion pound digital advertising industry that we are all a part of. Publishers and content creators sit at the heart of our industry and we have a responsibility to ensure that we protect and support a sustainable future for quality journalism.

A key media priority for advertisers is brand safety. This is a priority across all media channels, but digital advertising, with automated buying and an ever-changing environment, presents specific challenges for advertisers.

Content verification technologies emerged to help with managing brand safety online and play a crucial role in giving advertisers a layer of trust when investing in digital advertising. They provide a useful route to manage the scale of automated media environments. However, they need fine programming and skilled management for both advertisers and publishers to fully benefit from optimised brand safe environments. Misuse or overzealous use of such technology can lead to reduced reach and scale for advertisers, and a loss of revenue for publishers, overall hindering the sustainability of our industry.

The longevity and sustainability of our industry works in all our best interests, so the AOP, IAB UK, IPA, ISBA, JICWEBs and Newsworks, along with our members, have come together to create best practice guidelines when using content verification technology.

We’d like to say a special thanks to the content verification technology providers that have contributed to this paper.
“'Brand Safety’ describes the controls that companies in the digital advertising supply chain employ to protect brands against negative impacts to the brand’s consumer reputation”. TAG.

Brand safety is defined differently depending on the brand; for the purpose of this document we are referring to brand safety as the controls in place to avoid advertising from appearing against inappropriate or illegal content. By its nature, what is considered as ‘brand safe’ content differs for each brand as an environment that is safe for one may not be suitable for another. For example, think of a family friendly FMCG brand versus a hard spirit, alcohol brand - the environments considered safe for two such differing brands would vary vastly.

Who is responsible for brand safety?

From the advertiser defining what is safe or unsafe for their brand, to the intermediaries responsible for delivering ads, all the way to the publishers maintaining high editorial standards, not publishing fake news and maintaining trust with their readers - we all have a part to play to keep brands safe online.

Automated solutions have been developed to help deliver brand safety requirements, but they do not replace the need or importance of human input.
Brand safety today is managed in various ways, most commonly through the use of exclusion lists, inclusion lists and by using content verification technology.

**Exclusion Lists**

Sometimes called a ‘blacklist’ or ‘block list’. An exclusion is a list of terms e.g. words or URLs that are explicitly blocked. For the case of advertisers, an exclusion list could be a list of URLs that they do not want to appear on and for publishers it could be a list of advertisers that they do not want appearing on their website.

For your exclusion list, we recommend that you include websites listed on PIPCU’s Infringing Website List (IWL) and to exclude entities listed on the IAB/ABC Spiders and Bots list.

**Inclusion Lists**

Sometimes called a ‘whitelist’. An inclusion list is a list of terms e.g. words or URLs that are exclusively included. If it’s not on the list then it’s not included. In the case of advertisers, an inclusion list could be a list of URLs that the advertiser approves serving ads on. Any URL that is not on the list will be excluded by default. For publishers, an inclusion may be a list of advertisers they will work with.

Inclusion lists are typically more restrictive than exclusion lists because they exclude anything outside of a defined list. For anyone using inclusion lists, ensure that you are aware of the limitation to scale that may arise if you’re only employing this strategy.

**Content Verification Technology**

Content verification technology is used to recognise and categorise the content of an individual webpage. Publishers use this technology to categorise the content of their webpages and better package their inventory, while advertisers use it as an independent verification tool to check that brand safety requirements are being met by their media partners (e.g. not serving ads outside of exclusion or inclusion lists). In addition to verification, these technologies are able to assess the brand safety risk of content on a webpage, allowing advertisers to manage which environments their brand messaging appears in.

Nowadays, companies who offer content verification technology may also offer other services such as ad fraud protection and viewability measurement. However, for the purposes of this brand safety paper, we will be looking at the content verification technology in isolation.

Content verification technology is very sophisticated. However, as described earlier in the paper, misuse of such technology can have negative effects. For example, overzealous blocking will impact an advertiser’s reach, scale and costs, as well as hinder a publisher’s ability to monetise their inventory with digital advertising. It is therefore important that when such technology is used, it is applied effectively and does not block content unnecessarily. Later in this paper we set out some best practice guidance, principles and questions you should be asking when using such technologies.
There are various brand safety certifications and accreditations that advertisers should be aware of when choosing partners. Below is a summary of these certifications and who they apply to.

**IPSO, Editors’ Code** - IPSO’s Editor’s Code sets editorial standards that members of the press subscribe to and upkeep. The code balances both the rights of the individual and the public’s right to know. IPSO’s Editors’ Code is a certification for news and magazine publishers.

**JICWEBS DTSG** - The DTSG principles are guidelines aimed at significantly reducing the risk of ad misplacement of advertising and make public the processes individual companies undertake to approach brand safety. Companies’ brand safety processes are audited by a third-party and the certifications and audit notes are publicly available on the JICWEBS website.

All company types are applicable for the JICWEBS DTSG certification.

**JICWEBS CV Tools** - The Content Verification Tools certification sets out the minimum technical standards required of such technologies. Certified technologies have been audited by a third-party and have proven that they meet these minimum requirements. You can learn more about the standards set for these technologies [here](#). The JICWEBS CV Tools certification is for content verification technology providers.
Approaching Brand Safety

As laid out earlier in the paper there are various tools that can help protect a brand when serving ads online, however brand safety should be considered from the start of the campaign planning, as opposed to bolting on precautionary measures at the end.

Brand safety should be factored in from as early as when you are choosing how you will be buying your inventory i.e. from the publisher directly, through a private marketplace or through the open exchange.

Different inventory and different buying models offer different levels of transparency and control over the contextual environments where ads will be displayed.

There is a diminishing scale of insight when you move from serving ads on a single website to serving on multiple websites; and when moving from direct to indirect buying models. For example, consider a direct buy with a publisher who owns all content creation and exercises full editorial control. Then compare this to when buying on the open exchange across several inventory aggregators, which include non-curated and user generated content. In the former, you have more transparency and control of the environment your ad will appear in compared to the latter, and your brand safety measures should be adjusted accordingly.

The buying model (direct buy, private marketplace or open exchange) should be selected based on the advertiser's goals and attitude to risk. It logically follows that brand safety control becomes more important as the lack of insight or confidence around the contextual quality of content increases and the use of content verification technology should be scaled accordingly. For example, depending on the buyer's standards, a direct buy may require minimal content verification technology controls because they will be dealing directly with their intended publisher. Private marketplace buys may require additional content verification technology to monitor and confirm a buy was placed with the intended partner(s). In the open exchange, pre-bid technology may be utilised to prevent bidding on non-brand safe impressions and help minimise impression waste.

Additionally, the type of content that needs to be monitored or blocked may also need to be scaled according to the buying model being used. For example, you may only want to target away from illegal content e.g. IP infringing or hate speech content in private marketplace when you know the publishers you are buying from. However, when buying in the open exchange, where there are a variety of publishers selling their inventory, you may need to target away from all types of content deemed unsuitable for your brand.

When using any brand safety management tools, including content verification technology, there are trade-offs between scale, reach, cost and quality. These must be considered against overall campaign objectives and can lead to revised and updated use of content verification technology.

Overall, brand safety should be approached in a layered manner and taken into consideration from the start of campaign planning. First, there should be an informed buying model, then there should be the use of baseline inclusion or exclusion controls (either supported or offered by the publisher or buying platform), and then finally the use of additional controls via content verification technology.
Applying Content Verification

Content verification technology has come a long way since its first inception. From previously only being able to recognise keywords, these technologies are nowadays able to use proprietary methodologies and AI (such as ‘natural language processing’) to understand the content and context of webpages and categorise accordingly. This is called semantics analysis.

Semantics analysis can be a more effective way to manage brand safety over keyword blocking, as there are less risks of content being misinterpreted. Semantics analysis therefore helps to deliver brand safe environments without unnecessarily cutting down reach and scale. To reap the benefits, users of content verification technology should understand how their chosen vendor’s technology works to make sure they are using it most effectively.

For example, if you want to protect your brand from appearing against adult content, is there a specific category or setting you should be selecting? And if so, is it still necessary for you to include words like “sex” as part of your keyword blocking or would such content already be blocked by selecting that respective category?

The answer to this may vary depending on the technology you’re using. We recommend working closely with your chosen partner to ensure you understand and implement their technology correctly. Some questions you should be asking your content verification providers to inform your strategy, are as below.
Questions for Content Verification Providers

Here are some questions that you should be asking your content verification providers:

• What channels and formats are you able to measure with your technology?
• What is your technology able to measure i.e. brand safety, fraud, viewability, audience etc.?
• What methods do you use to analyse content? Is this the same across all your service offerings?
• Does your content offer multi-language capabilities?
• Are you able to classify content beyond text (e.g. video or images)?
• Do you have the ability to block ads or are you monitoring only?

• Do I have to pay for blocked impressions?
• When blocking, what data-points are you evaluating?
• If an impression is blocked, what information do I have access to about why?
  » Do the publishers/agencies have access to the same data that I do?
  » How are these recorded in my ad server vs. the publisher’s ad server?
• Will you tell my publishers the campaign monitoring and blocking settings at the start of the campaign? Should I do this?
• Have you been accredited by any governing bodies such as JICWEBS? Are any of the numbers in your reporting not accredited?
Best Practice: Keyword Blocking

Keyword blocking is a brand safety tool used to help minimise the risk of an ad appearing against content that may be unsafe for the advertiser. It is a blunt tool that recognises a list of words the user has deemed to be unsafe and blocks a brand’s ads from appearing in any environments where that word appears, regardless of the context it is being used in.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Context intended to be blocked</th>
<th>Examples of other contexts being inadvertently blocked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shot</td>
<td>Crime/Death &amp; Injury</td>
<td>Sport, Fashion, Medicine</td>
</tr>
<tr>
<td>Strip</td>
<td>Adult</td>
<td>DIY, Sport</td>
</tr>
<tr>
<td>Manchester</td>
<td>Terrorism</td>
<td>Sport, Travel, News</td>
</tr>
<tr>
<td>Ariana Grande</td>
<td>Terrorism</td>
<td>Music, News</td>
</tr>
<tr>
<td>Attack</td>
<td>Crime/Death &amp; Injury</td>
<td>Sport</td>
</tr>
<tr>
<td>Fight</td>
<td>Crime/Death &amp; Injury</td>
<td>Sport, Health &amp; Beauty (‘fight the signs of aging’)</td>
</tr>
<tr>
<td>Diesel</td>
<td>Environment</td>
<td>Automotive</td>
</tr>
</tbody>
</table>

The screenshots on the next page show real life examples of the types of content that are being blocked by keyword blocklists today.
Best Practice: Keyword Blocking

Sensitive category incorrectly assigned: Hate speech

Sensitive category incorrectly assigned: Crime / Death & Injury

Sensitive category incorrectly assigned: Crime / Child Abuse / Sexual Offence

Sensitive category incorrectly assigned: Adult
Best Practice: Keyword Blocking

Best practices when using keyword blocking

Used on its own, keyword blocking could be ineffective and should be considered in line with the overall approach and not as a default/‘always on’ choice. As stated previously, there are different buying models, exclusion lists, inclusion lists and semantics analysis that can all be used to manage brand safety. Therefore, application of keyword blocklists should be aligned to the respective risk.

The greater number of controls in place, the greater the impact on the scale, reach, cost and quantity trade off. Therefore, adding a keyword blocklist in addition to all other controls will have an impact that should be carefully considered.

If the best option available is to use a keyword blocklist then careful thought should be given to its creation and to any updates. The list should not go beyond the brand safety layered approach that would be put in place if other controls were available, nor should it exceed the types of content that would be avoided if other controls were available. Instead, keyword blocklists should complement other layers of control in place, for example, only addressing gaps that are not fully covered by the categories you are choosing to avoid.

Best practice includes:

- Starting with a concise set of keywords deemed unsuitable by your brand
- Reviewing whether these keywords are appropriate to the level of brand safety in place and address only the types of content to be avoided
- Customising for brand specific requirements, for example to address known negative PR topics
- Asking “would blocking this keyword prevent my ad from also appearing alongside any safe content?” and adjusting appropriately
- Not using a one-size-fits-all and all-risk encompassing list
- Not adopting a past list
- Setting a regular review cadence and ensuring clear ownership of changes
- If used to address a public crisis or negative PR issue, ensure these specific terms are part of the review cadence
- Understand the trade-offs across scale, reach, cost and quality of using excessive lists and the risk of blocking safe content
Crisis Management

In this scenario, there will never be a 100% fail safe solution. Therefore, any brand safety strategy should include an incident response process to address issues quickly, to course correct and to avoid any reoccurrence. At a minimum, the strategy should include clear direction on:

• Who is responsible for managing the issue across the advertiser, agency, verification technology, ad serving/buying technology and media side?
• Who is the final decision-maker?
• What are the timelines for decision-making?

There will always be a range of options:

• For breaking news stories, editorial controls may already block advertising from appearing, therefore confirmation from media and verification partners may be all that is needed as part of the crisis management response
• For issues on a specific site, an update to an exclusion list may be required. This could be temporary if you’re able to work directly with the media partners, or longer term if there is no direct relationship
• For a “new” brand safety requirement – for example non-harmful content attracting paedophile attention – the solution may be to implement an existing content type blocking category via verification technology
• For a “new” brand safety trend – for example children eating Tide pods for a challenge – the solution may be to work with verification technology to create a specific content category or manage through a keyword blacklist update of a specific term, understanding that by choosing to block against the word “Tide”, safe impressions would undoubtedly be missed

The plan should be well documented internally to avoid any panic and rash decision-making. There also always remains the option to pause ad campaigns to take time to fully assess the scale of the public or PR issue.

Once action has been taken, all actions should be reviewed to confirm whether they need to be temporary while the issue is resolved, or longer term if the brand safety risk is deemed to be ongoing and not addressable.

The crisis management approach should be aligned to the buying approach and, as methods move away from single and direct buying relationships and/or towards more aggregated and indirect methods, the effective action will often need to be one of the more wide-ranging rather than targeted options.
The Loss to Advertisers

This guide addresses the sustainability of digital advertising and the long term impact content blocking is having on publishers and quality journalism. It is equally important that we highlight the losses to advertisers from overusing content blocking and keyword blocking in the form of lost reach, scale and increased costs. Take a look at the following case studies and examples for evidence of the effects on advertisers.

Case study from DoubleVerify

A European luxury advertiser had a keyword list of over 400 words and phrases. By working with its verification provider to understand how keyword blocking works and to understand the coverage already provided by content avoidance categories, it was able to reduce the list down to 12 keywords, which led to a keyword block rate reduction of over 97%. This action resulted in thousands of pounds in media savings, which would have been wasted due to unnecessary and out-of-date keywords blocking its already-paid-for programmatic impressions.

When the advertiser realised that many of its keywords were already covered under content categories and that repeating them on the keyword blocklist was resulting in false-positives, it removed them from the blocklist. By doing so, the block rate dropped, which meant that the media it was winning the bids for was serving as opposed to being blocked.

Data analysis from Reach Plc

Reach Plc pulled some data to show the number of pages potentially being blocked by using keyword blocking.

This data is based on Reach Plc’s domains only and looks at data from one day.

Reach looked at the impact of three keywords commonly found on brand blocklists – ‘Manchester’, ‘Shot’ and ‘Strip’. It found that, of the 36,667 articles that were read by users across Reach Plc’s domains on 10 January 2020, 2,905 of the URLs included one or more of the three keywords on the advertisers blocklist (“Manchester”, “shot” and “strip”).

Therefore, if an advertiser were using technology that does keyword blocking based on the URL, these 3,000 URLs would be blocked. This accounts for 8% of all URLs read on this day. This does not account for how many times these pages were viewed and how many impressions this would account for.

On the same day, Reach Plc published 2,951 new articles; 446 of these articles included one or more of the three keywords within the body of the article. This means that any tool blocking keywords based on the words in the body of a webpage would block over 15% of all the new articles published on that date. Again, this does not account for the number of times these pages were viewed and the number of missed impressions. When Reach scanned these 446 articles using Mantis, its new brand safety product, it found that 89% of them were brand safe.
Consumer Perspective

Brand safety has been a hot topic for online advertising since The Times’ investigation in February 2017 discovered that big brands were unwittingly funding terrorism, supremacism and pornography via advertising on sites and videos. Programmatic systems have developed tactics like blacklisting, whitelisting and keyword blocklists to avoid dangerous sites and content. However, whether intentionally (some brands avoid running against “hard news” online when they don’t in printed newspapers, TV or radio) or as an unintended consequence of blocking, content that can provide great reach, engaged audiences and contextual relevance is being shunned. In some ways, it is the opposite to the usual approach to newspaper advertising, where being near the front of the paper has traditionally been seen as very desirable. And of course, the front of the paper is most likely to have the hard news stories – with the possible exception of royal babies!

So, in light of the questions around brand safety online, Newsworks set out to explore whether there was a difference in responses to advertising in hard and soft news contexts. The research, conducted by Neuro-Insight, used neuroscience to measure unconscious brain responses and more traditional quantitative and qualitative techniques to capture the conscious attitudes of readers.
Consumer Perspective

Key findings
At a conscious level, readers can easily distinguish between hard and soft news stories and describe the feelings that are provoked. They appreciate the value of both. However, they also understand the role and value of news brands:

• 86% agree that they know that the role of news brands is to “keep me up-to-date with all kinds of stories and that sometimes they can be upsetting or shocking”

• 89% “like browsing my news brand and coming across new things”

• Although some people prefer ads in a soft news context, others feel that ads in a hard news story are more trusted

Brain response is very similar for hard and soft news stories. There is no increased withdrawal from hard news, whether that be in print or online. In fact, the research shows higher initial levels of brain activity for hard news as people are engaged with the story.

Neuroscience results also indicate that a hard news environment delivers an incremental benefit to advertisers. It has no negative impact on advertising responses:

• Average ad dwell time is 1.4 times higher in a hard news environment (45 seconds vs 32 seconds in a soft news environment)

• While the average levels of response to ads in hard and soft news environments are similar, the pattern of response shows more and stronger peaks for ads in a hard news environment. This indicates that the brain is more actively engaged and there is more likelihood of key messages being encoded into memory

• Ads in both hard and soft news environments deliver strong engagement (personal relevance), emotional intensity and, most importantly, elicit strong levels of memory encoding

In conclusion, there is no evidence that hard news damages advertiser brands. The research demonstrates that the news environment creates high engagement for advertisers in both hard and soft news contexts. As an industry, we need to develop more intelligent ways of defining brand safety standards so that we can accentuate the positive benefits.
Brand Safety Checklist

- What environments are unsafe for the brand to appear against?
  » Have I clearly communicated this to all relevant parties?

- Do I have the right buying model for my campaign given the risk adversity of the brand?

- Do I need to layer any exclusion or inclusion lists?
  » What restrictions arise from implementing this list? How will my reach and scale be affected?

- Do I need to work with a content verification provider?
  If yes...
  » Do I understand my vendor’s technology?
  » Should I be monitoring or blocking?
  » Have I communicated my brand safety requirements to this vendor?
  » Are all my brand safety requirements covered by the vendors categories?
  » Do I require any custom categories?

- Are there any brand safety concerns not being covered by my brand safety settings?
  » If so, can they be addressed by scaling the existing settings?

- Do I need to layer any keyword blocking?
  » If yes, use the Keyword Blocking Best Practice Guidance when putting this together
Creating a safe online environment for brands is in all of our interests and every part of the digital ad industry has a role to play in ensuring this. In order to minimise brand safety risks without damaging advertisers’ reach and scale opportunities, a sophisticated and nuanced application of the tools available is required. Crucially, there is no one-size-fits-all solution, with brands needing to individually establish the level of safety measures necessary and tailoring their approach accordingly.

However, as this guide has detailed, there are core factors that need to be considered when implementing a brand safety strategy:

• Misuse or overzealous use of content blocking can be damaging for both brands and publishers. Brands limit their reach by ruling out safe environments and publishers struggle to monetise their content.

• Brand safety considerations need to be factored in from the start of campaign planning, as early as when choosing a buying model.

• Keyword blocking is a blunt tool that doesn’t take into consideration context. The effects of it should be carefully considered before it’s applied.

• Alternatively, semantics analysis is a more effective way of managing content blocking compared to keyword blocking. To benefit from this technology, you need to have a good understanding of how your partner’s technology works.

• Being in a hard news environment is not necessarily detrimental to your brand, with research showing that brain response is very similar for hard and soft news stories. In fact, a hard news environment delivers higher dwell times and higher potential for memory encoding.

By taking on board the advice in this guide, we can build a more contextual system of content verification that supports brands, publishers and the functionality of our ad-funded web.

We’d like to say thank you to all our contributors and working group:

Amazon  AOP  COTY
Google  GroupM  Hearst
IAB UK  Integral Ad Science  IPA
ISBA  JICWEBS  Mail Metro Media
News UK  Newsworks  Oracle
Reach Plc  The Guardian  the7stars

Information correct at time of printing.