



Australian Code of Practice  
on Disinformation and  
Misinformation  
Microsoft and LinkedIn  
Annual Transparency Report  
May 2023

## Summary

Microsoft is pleased to file this report on our commitments under the Australian Voluntary Code of Practice on Disinformation and Misinformation, covering the reporting period of calendar year 2022.

At Microsoft, we are committed to instilling trust and security across our products and services, and across the broader web, as outlined in our 2021 and 2022 Transparency Reports under the Code. We continue to recognise that fighting disinformation is a key element to creating a trustworthy and safe online environment and continue to increase our efforts to counter these threats.

We also recognise that there is not a one size fits all approach to this work, and instead there needs to be a whole of society strategy that recognises that not all people or platforms are the same and that different measures may be more effective than others in improving the information environment for all our users.

The Microsoft services in scope of the Voluntary Code are:

- **Microsoft Advertising:** Microsoft's proprietary online advertising network, which serves the vast majority of ads displayed on Bing Search and provides advertising to most other Microsoft services that display ads.
- **Bing Search:** a web search engine which provides a variety of services including web, video, image, and map search products. Bing Search does not host the content appearing in search results, does not control the operation or design of the indexed websites and has no ability to control what indexed websites publish. The reporting period does not cover Bing Chat, which was released in February 2023.
- **Microsoft Start:** a service which delivers licenced news and content across web and mobile for Microsoft customers and syndication partners.
- **LinkedIn:** a real identity online social networking service for professionals to connect and interact with other professionals, to grow their professional network and brand, and to seek career development opportunities. It operates via websites and mobile apps and includes user-generated content.

In June 2022, Microsoft announced the first [Information Integrity Principles](#). These principles were adopted across all impacted Microsoft products and teams to ensure an enterprise approach to information integrity while also recognising the immense diversity across the company. These principles establish a foundational set of commitments that teams can use to inform their policy, product development and risk assessment work. The four information integrity principles are:

- **Freedom of Expression:** We will respect freedom of expression and uphold our customers' ability to create, publish, and search for information via our platforms, products, and services.
- **Authoritative Content:** We will prioritise surfacing content to counter foreign cyber influence operations by utilising internal and trusted third-party data on our products.

- **Demonetisation:** We will not wilfully profit from foreign cyber influence content or actors.
- **Proactive Efforts:** We will proactively work to prevent our platforms and products from being used to amplify foreign cyber influence sites and content.

### **Immediate response to Russia's invasion of Ukraine, February 2022**

As published on our [Microsoft On the Issues blog](#), in response to the invasion of Ukraine in 2022, we swiftly moved to reduce the exposure of Russian state propaganda, as well to ensure our own platforms do not inadvertently fund these operations. This has included:

- not displaying any Russia Today (RT) and Sputnik content in Microsoft Start;
- removing RT news apps from our Windows app store;
- further de-ranking RT and Sputnik news sites' search results on Bing Search so that it will only return links when a user clearly intends to navigate to those pages; and
- banning all advertisements from RT and Sputnik across our ad network and not placing any ads from our ad network on these sites.

These actions were taken across the Australian versions of our services and services available to Australians.

During the reporting period, Microsoft took urgent and extraordinary steps in response to the war in Ukraine. In June 2022, Microsoft released a report entitled "[Defending Ukraine: Early Lessons from the Cyber War](#)". The report exposed the expansive cyber war, both cyber-attacks and information operations, that Russia is pursuing against Ukraine and its allies. In a follow up blog post released in December 2022, Microsoft further outlined Russian cyber operations including influence operations looking to leverage energy and food supply concerns across Europe to weaken the alliance against the Russian invasion. To address these threats, Microsoft developed a whole of society approach to mitigate the risk of foreign information operations:

- **Detect:** Collectively hunt, track, and investigate foreign perpetrators of disinformation—much like is done for foreign cyber actors. Pull together disparate efforts, often operating in company silos, and not integrated into the broader cybersecurity community.
- **Disrupt:** Leverage threat intelligence to disrupt operations, much like the successful takedown of ransomware operators. In addition to operation disruptions, it's essential to choke off the financial supply to known foreign disinformation sites, whether via ad placements, traffic sources, or otherwise.
- **Defend:** Build consumer facing technology with information integrity as a key principle. Foster innovation and research to enable more responsible technology. Build a more resilient society through programs and technology that encourage critical news consumption.
- **Deter:** Secure international norms that create a standard of behaviour for nation-state information campaigns, particularly for those that touch on topics involving fundamental human rights, such as healthcare.



Along with these new strategies, in July 2022, Microsoft announced the acquisition of Miburo Solutions, a cyber threat analysis and research company specialising in the detection of and response to foreign information influence operations. Working in close collaboration with the Microsoft Threat Intelligence Center (MSTIC), the new Microsoft Digital Threat Analysis Center (DTAC) has enabled Microsoft to expand its threat detection and analysis capabilities to shed light on the ways in which foreign actors use information operations in conjunction with cyber-attacks to achieve their objectives.

At Microsoft, we believe that the electoral process should be open and secure. In 2018, Microsoft launched the **Democracy Forward Initiative** (previously known as the Defending Democracy Program) to coordinate and track the work undertaken across the company on protecting and strengthening democratic institutions. The Democracy Forward team leverages Microsoft's role as a business and software provider to increase our clients' and users' ability to counter external efforts that compromise a healthy information ecosystem.

Microsoft is an inaugural signatory to the Electoral Council of Australia and New Zealand (ECANZ) Statement of Intent with Online Platforms, designed to support Australian electoral management bodies and online platforms to work together to promote and support the integrity of electoral events in Australia. During the reporting period, Microsoft worked closely with both the Australian Electoral Commission and the Victorian Electoral Commission to establish arrangements to manage content referrals related to breaches of the relevant electoral laws and our relevant terms of service. Neither Microsoft Advertising nor LinkedIn accept political advertising.

In addition to adhering to our obligations under Australian law, Microsoft strives to provide our customers a positive online experience free from deceptive advertisements. Microsoft is working across our services to achieve this goal through policies and enforcement processes aimed at ensuring that the advertising and content served is clear, truthful, and accurate. All of Microsoft's services that display advertising have adopted and vigorously enforce policies prohibiting disinformation.

Microsoft's company-wide commitment to disrupting the economics of disinformation is well-illustrated by **Microsoft Advertising**. Microsoft Advertising works both with advertisers, who provide it with advertising content, and publishers, such as Bing Search, who display these advertisements on their services. Microsoft Advertising employs a distinct set of policies and enforcement measures with respect to each of these two categories of business partners to prevent the spread of disinformation through advertising.

In 2022, Microsoft Advertising took down more than 7 billion ads and product offers globally for various policy violations. We have scaled up our Advertiser Identity Verification program from 7 pilot markets in 2021 to over 100 markets in 2022, including Australia. This program fosters our efforts to show advertisements from trusted sources by requiring advertisers to establish their identity as a business or as an individual.



**Bing Search** is an online search engine with the primary objective of connecting users with the most relevant search results from the web. Users come to Bing with a specific research topic in mind and expect Bing to provide links to the most relevant and authoritative third-party websites on the internet that are responsive to their search terms. Therefore, addressing misinformation in organic search results often requires a different approach than may be appropriate for other types of online services. Blocking content in organic search results based solely on the truth or falsity of the content can raise significant concerns relating to fundamental rights of freedom of expression and the freedom to receive and impart information.

Instead of blocking access to content, Bing focuses on ranking its organic search results so that trusted, authoritative news and information appears first and provides tools to help its users evaluate the trustworthiness of certain sites and ensure they are not misled or harmed by the content that appears in search results.

**LinkedIn** is a real identity online social networking service for professionals to connect and interact with other professionals, to grow their professional network and brand, and to seek career development opportunities.

LinkedIn is part of its members' professional identity and has a specific purpose. Activity on the platform and content members share can be seen by current and future employers, colleagues, potential business partners and recruitment firms, among others. Given this audience, members largely limit their activity to professional areas of interest and expect the content they see to be professional in nature.

LinkedIn is committed to keeping its platform safe, trusted, and professional, and respects the laws that apply to its services. On joining LinkedIn, members agree to abide by LinkedIn's [User Agreement](#) and its [Professional Community Policies](#), which expressly forbid members from posting information that is intentionally deceptive or misleading.

When LinkedIn sees content or behaviour that violates its Professional Community Policies, it takes action, including the removal of content or the restriction of an account for repeated abusive behaviour. In 2022, LinkedIn globally blocked more than 80 million fake accounts and removed more than 310,000 pieces of misinformation. Over the same period, LinkedIn blocked more than 411,000 fake accounts attributed to Australia and removed approximately 5,600 pieces of misinformation reported, posted, or shared by Australian members.

**Microsoft Start** is a personalised feed of news and informational content from publishers available in a number of Microsoft products, including a standalone website (MSN.com), a mobile app on both Android and iOS, the News and Interests experience on the Windows 10 taskbar, the Widgets experience in Windows 11, and the Microsoft Edge new tab page.

On Microsoft Start, we have policies to specifically address disinformation and misinformation on clear and well-defined misinformation narratives, including the Russia-Ukraine conflict which was introduced in February 2022. Topics are chosen based on the



potential for real-world harm and the perniciousness of their spread across the globe. Microsoft Start has also addressed violations to our community guidelines through takedowns.

Unless otherwise specified, data provided is for 2022 calendar year.

## Commitments under the Code

Commitment	Relevant Microsoft service
1a: Contribute to reducing risk of harm by adopting scalable measures	Bing Search, Microsoft Start, Microsoft Advertising, LinkedIn
1b: Users informed about types of behaviours and content prohibited/managed	Microsoft Start, Microsoft Advertising, LinkedIn
1c: Users can report content that violates policy through accessible reporting tools	Bing Search, Microsoft Start, Microsoft Advertising, LinkedIn
1d: Users can access general information about response	Bing Search, Microsoft Start, Microsoft Advertising, LinkedIn
2: Advertising and/or monetisation incentives reduced	Microsoft Advertising, LinkedIn
3: Risk of inauthentic behaviours undermining integrity and security of services/products reduced	Bing Search, Microsoft Advertising, LinkedIn
4: Users more enabled to make informed choices about sources of news and factual content and to identify misinformation	Bing Search, Microsoft Start, LinkedIn
5: Users better informed about source of Political Advertising	Microsoft Advertising, LinkedIn
6: Support efforts of independent research	Microsoft
7: Public access to measures to combat disinformation and misinformation	Bing Search, Microsoft Start, Microsoft Advertising, LinkedIn

## Reporting Against Commitments

### Objective 1: Safeguards against Disinformation and Misinformation

Outcome 1a: Signatories contribute to reducing the risk of harms that may arise from the propagation of Disinformation and Misinformation on digital platforms by adopting a range of scalable measures.

Microsoft reduces the risk of harms that may arise from the propagation of disinformation and misinformation on **Bing Search, Microsoft Start, Microsoft Advertising** and **LinkedIn** through the application of our internal policies and scalable measures.

## Bing Search

**Bing Search** is an online search engine that provides a searchable index of websites available on the internet. Bing Search does not have a news feed for users, allow users to post and share content, or otherwise enable content to go “viral”. Nonetheless, disinformation may at times appear in both organic and paid search results, and we take active steps to counter it. As emphasised in the summary above, addressing disinformation in organic search results often requires a different approach than may be appropriate for other types of online services, such as social media services.

Bing Search’s primary mechanism for combatting misinformation in search is via ranking improvements that take into account the quality and credibility (QC) of a website and work to rank higher quality and more authoritative pages over lower authority content. Bing Search’s ranking policies, including how QC is determined, are described in the How Bing Ranks Your Content section of the [Bing Webmaster Guidelines](#). Bing Search’s general spam policies also prohibit certain practices intended to manipulate or deceive the Bing Search algorithm, including techniques employed by malicious actors in the spread of misinformation. Bing’s spam policies are detailed in the “Abuse and Examples of Things to Avoid” section of the Bing Webmaster Guidelines. Pursuant to the Webmaster Guidelines, Bing may take action on websites employing spam tactics or that otherwise violate the Webmaster Guidelines, including by applying ranking penalties (such as demoting a website) or delisting a website from the index.

Although the Bing Search algorithm endeavours to prioritise relevance, quality, and credibility in all scenarios, in some cases Bing Search identifies a threat that undermines the efficacy of its algorithms. When this happens, Bing Search employs “defensive search” strategies and interventions to counteract threats. Bing Search implements tactics, techniques and procedures in accordance with its trustworthy search principles in order to protect Bing Search users:

- from being misled by untrustworthy search results; and/or
- inadvertently being exposed to unexpected harmful or offensive content.

Defensive search interventions may include:

- algorithmic interventions (such as quality and credibility boosts or demotions of a website);
- restricting autosuggest or related search terms to avoid directing users to problematic queries; and
- manual interventions for individual reported issues or broader areas more prone to misinformation or disinformation (e.g., elections, pharmaceutical drugs, or COVID-19).

### Defensive Search Interventions, Australia, January – December 2022

	Queries	Impressions
<b>Total</b>	64,104	4,441,099
<b>Ukraine related<sup>#</sup></b>	45,100	1,072,939

<sup>#</sup>Ukraine data from February to December 2022



While Bing Search generally strives to rank its organic search results so that trusted, authoritative news and information appear first and provides tools that help Bing Search users evaluate the trustworthiness of certain sites, we also believe that enabling users to find all types of information through a search engine can provide important public benefits. In addition, Bing users have many legitimate reasons for seeking out content in search that may be harmful or offensive in other contexts (such as for research purposes).

Bing regularly partners with independent research and non-profit organisations to maintain threat intelligence and inform potential algorithmic interventions. Bing Search also takes action to remove autosuggest and related search terms that have been found likely to lead users to low authority content. Bing Search also may include answers or public service announcements at the top of search results pointing users to high authority information on a searched topic or warnings on particular URLs known to contain harmful information (such as unaccredited online pharmacies and sites containing malware).

Where circumstances warrant (such as public health crises or major elections), Bing Search may provide information hubs for users to easily access a centralised repository of high authority information.

For example, in response to the COVID-19 pandemic, Bing Search introduced multiple methods to promote reliable content for Australian users, including:

- launching a specialised COVID-19 information hub providing centralised news and country-specific data related to the pandemic, including case rates, vaccine data, and COVID-19 related news;
- providing reliable health information through public service announcements pointing to authoritative third-party sources of health information (e.g., the US Center For Disease Control and the World Health Organization) for certain COVID-19 queries, such as for queries seeking information about COVID-19 symptoms; and
- placing reliable information near the top of search results pages and in sidebar windows

As another example, in response to Russia's invasion of Ukraine in February 2022, Bing Search has continued to monitor potential threats and promote authoritative content related to the conflict. Bing Search has taken steps to algorithmically boost authority signals and employ defensive search interventions in relation to the conflict. From February 2022 through 31 December 2022, Bing Search deployed algorithmic interventions on over 45,000 distinct queries impacting over one million impressions to avoid users being exposed to less authoritative information in Australia.

### **Microsoft Start**

**Microsoft Start** delivers high-quality news across web and mobile experiences for Microsoft as well as a growing number of syndication partners. Microsoft Start's model reduces risk of disinformation and misinformation being propagated. Misinformation in our licenced content feed has been exceedingly rare.





- Our content providers are vetted and must adhere to a strict set of standards that prohibit false information, propaganda and deliberate misinformation.
- Microsoft Start is free to download, with no limits on number of articles or videos a user can view.

Microsoft Start Community was introduced in September 2020 and launched in Australia in May 2021. It supports diverse, authentic conversations and content about issues and events. This is a safe, inclusive, and respectful forum where participants are responsible for their posts and how they treat one another. Our [Community Guidelines](#) are designed to uphold these values and we strive to provide transparency and clear guidance on how to comply with them.

- If a contribution is flagged, it will be reviewed. If it does not meet the community guidelines it will be removed.
- User activity feed shows if any comments have been removed and users are able to appeal the decision.

When necessary, Microsoft Start will suspend a user’s ability to comment. Continued refusal to meet standards may result in permanent ban, which users have an opportunity to appeal. The Comments function was relatively nascent during the reporting period.

A misinformation trait will define what can and cannot be said on our platform about a particular topic. We have specific policies for managing misinformation relating to well-defined misinformation narratives with potential for real-world harm - which includes disabling comments for certain articles to reduce propagation of disinformation.

- During the reporting period, we introduced misinformation traits related to issues that are specific to a particular market or event, adding to the COVID-19 and QAnon traits introduced in 2021.
- In response to the invasion of Ukraine in February 2022, we quickly developed and published a misinformation trait to prevent the Microsoft Start Community from becoming a platform for disinformation.

### Microsoft Start Comments, Australia Takedowns, October 2021 – December 2022

	October – December 2021 <sup>#</sup>		January - December 2022	
Total takedowns	<b>73,700</b>	<b>100%</b>	<b>849,000</b>	<b>100%</b>
Misinformation – all <sup>*</sup>	1,899	2.5%	9,256	1.09%
Misinformation – COVID	1,810	2.4%	8,655	1.01%
Misinformation - QAnon	89	0.12%	425	0.05%
Misinformation - Russia/Ukraine <sup>^</sup>			128	0.01%

<sup>#</sup>Comments data prior to October 2021 is not a reliable metric as the function was only in its early stages.

<sup>\*</sup> Misinformation total includes comments which have more than one trait labelled; percentages are rounded; sub-category list is not exhaustive.

<sup>^</sup>Russia/Ukraine misinformation trait was introduced in February 2022.

## Microsoft Advertising

Microsoft Advertising's [Misleading Content Policies](#) prohibit advertising content that is misleading, deceptive, fraudulent, or that can be harmful to its users, including advertisements that contain unsubstantiated claims, or that falsely claim or imply endorsements or affiliations with third party products, services, governmental entities, or organisations.

**In 2022, Microsoft Advertising took a number of actions to ensure a safe and trusted experience for users globally including:**

- taking down more than 7 billion ads and product offers for various policy violations, more than twice as many as in 2021. We suspended nearly 232,000 accounts and banned nearly 453,000 websites from our network;
- making use of significant advancements in artificial intelligence (AI) to quickly adapt to new patterns and methods used by bad actors;
- ensuring that our protection mechanism involved coverage for all types of content such as text, images, and videos to quickly detect malicious activity in our system;
- making advancements in our human moderation workflows to capture more insights from reviews, continuously improving our systems; and
- leveraging intelligent tools to allow our human reviewers to establish linkages between various accounts and discover fraud rings quickly and efficiently.

Microsoft Advertising also has a set of [Relevance and Quality Policies](#) to manage the relevancy and quality of the advertisements that it serves through its advertising network. These policies deter advertisers from luring users onto sites using questionable or misleading tactics (e.g., by prohibiting advertisements that lead users to sites that misrepresent the origin or intent of their content).

Under our [Sensitive Advertising Policies](#), Microsoft reserves the right to remove or limit advertising permanently or for a period of time in response to a sensitive tragedy, disaster, death or high profile news event, particularly if the advertising may appear to exploit events for commercial gain or may effect user safety.

Microsoft Advertising employs dedicated operational support and engineering resources to enforce these policies, combining automated and manual enforcement methods to prevent or take down advertisements that violate its policies. Every ad loaded into the Microsoft Advertising system is subject to these enforcement methods, which leverage machine-learning techniques, automated screening, the expertise of its operations team, and dedicated user safety experts. In addition, Microsoft Advertising conducts a manual review of all advertisements flagged to its customer support team and removes advertisements that violate its policies.

To respond to the COVID-19 pandemic, Microsoft Advertising takes action against advertisements that contain disinformation about COVID-19 through its policies, including



its misleading content policies which prohibits advertising that can reasonably be perceived as being deceptive, fraudulent or harmful to site visitors.

Based on this policy, at the onset of the COVID-19 crisis, we prohibited all advertising that sought to exploit the crisis for commercial gain, spread misinformation, or that may have posed a danger to user-health or safety. In addition, Microsoft Advertising:

- requires our publishing partners to abide by strict brand safety-oriented policies to avoid providing revenue streams to websites engaging in misleading, deceptive, harmful, or insensitive behaviours. These policies include a comprehensive list of prohibited content that our ads cannot serve against, including disinformation;
- requires publishers to maintain a list of prohibited terms and provide us with information on their content management practices where applicable;
- requires publishers to abide by restrictions against engaging in business practices that are harmful to users; and
- reviews publisher properties and domains for compliance with these restrictions and promptly notifies publishers of properties or domains that violate Microsoft Advertising's policies.

Microsoft does not approve properties that violate our policies for live ad traffic; if a property or domain that violates our policies is already live, we remove it from our ad network until the publisher remedies the issue. We also give advertisers the option to block their ads from being displayed on particular web domains.

Microsoft Advertising is preventing serving advertising related to the Ukraine crisis pursuant to its Sensitive Advertising Policies.

- Microsoft Advertising has not seen any significant traffic or recently received escalations or takedown requests related to the Ukrainian crisis.
- Microsoft Advertising banned all advertisements from state-sponsored media outlets associated to spreading disinformation, such as Russia Today (RT) and Sputnik, across our ad network and will not place any ads from our ad network on these sites.
- Since February 2022, we have blocked 2,321 domains from our network globally.

#### Microsoft Advertising Global Ad Takedowns

2020	2021	2022
1.6 billion	3 billion	7.2 billion

#### Microsoft Advertising Ad Safety in Australia

Action	2021		2022*	
	Global	Australia	Global	Australia
Rejections	3b	191m	7.2b	1b
Total appeals	72,413	7,025	127,158	14,536
Total appeals overturned	28,965	3,248	101,537	9,522

Total complaints	70,000	201	35,667	285
Complaint: Policy violation	20,934	68	1,156	57
Complaint: Trademark infringement	34,700	127	32,213	153
Complaint: User safety issues	416	5	1,805	58
Complaints: Other	13,950	69	493	17
Total entity takedowns	250,124	2,956	551,424	118,321
Average processing time	~36 hours	~36 hours	~36 hours	~36 hours

\* Although not possible to estimate with precision, the year-over-year growth in the number of rejections and related figures may be due to the expansion of Microsoft Advertising in new international markets, and the growth in adoption of certain advertising formats compared to the previous year.

We have expanded the Advertiser Identity Verification program from seven markets in 2021 to over 100 markets in 2022, including Australia. As at the end of the reporting period, just over 1,000 accounts have been included in the Advertiser Identity Verification pilot in Australia. Microsoft Advertising plans to complete the program roll out in 2023. The system enables customers to see ads from trusted sources. The selected advertisers are required to establish their identity as a business or as an individual by submitting all necessary information and documents.

Microsoft ensures that all advertisements on our services are clearly distinguishable from editorial or other non-sponsored content.

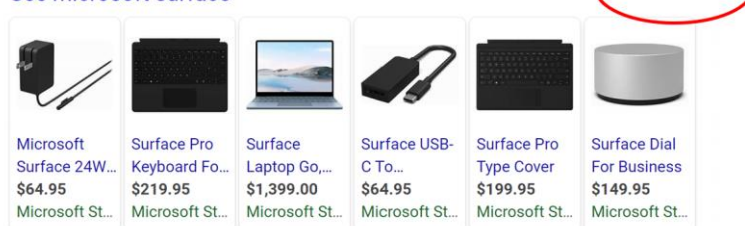
- For example, all Microsoft services that display ads served by Microsoft Advertising clearly distinguish sponsored from non-sponsored content by displaying an advertising label in a readily noticeable location on the page.
- An example of how ads are displayed is shown in red below. Clicking on the information icon or downward arrow next to an advertising label displays a click through to the ad setting page.

#### Surface Devices, Accessories - Microsoft Store

<https://www.microsoft.com/en-au/store/collections/surfacelist>

The most portable **Surface** touchscreen 2-in-1 is perfect for your everyday tasks, homework and play. Designed to light up the best of Windows 11, **Surface Go 3** is optimised for digital pen and...

See microsoft surface



The screenshot shows a grid of product cards for Surface devices and accessories. Above the grid, the text 'See microsoft surface' is followed by an 'Ads' label with a downward arrow icon, which is circled in red. The product cards include:

- Microsoft Surface 24W... \$64.95
- Surface Pro Keyboard Fo... \$219.95
- Surface Laptop Go... \$1,399.00
- Surface USB-C To... \$64.95
- Surface Pro Type Cover \$199.95
- Surface Dial For Business \$149.95

Microsoft Advertising similarly requires all its publishers to use a clear and prominent label indicating that the advertisements served by Microsoft Advertising on their properties are



sponsored. Microsoft Advertising proactively reviews publisher partners to enforce this requirement.

### **LinkedIn**

To help keep **LinkedIn** safe, trusted, and professional, our [Professional Community Policies](#) clearly detail the range of objectionable and harmful content that is not allowed on LinkedIn. Fake accounts, misinformation, and inauthentic content are not allowed, and we take active steps to remove it from our platform.

LinkedIn has automated defences to identify and prevent abuse, including inauthentic behaviour, such as spam, phishing and scams, duplicate accounts, fake accounts, and misinformation. Our Trust and Safety teams work every day to identify and restrict inauthentic activity. We're regularly rolling out scalable [technologies](#) like machine learning models to keep our platform safe.

Using the process described in response to Outcome1c below, LinkedIn members also can report content they believe violates our Professional Community Policies, including misinformation, inauthentic content, and fake accounts. If reported or flagged content violates the Professional Community Policies, it will be removed from the platform. We may also restrict the offending member's LinkedIn account, depending on the severity of the violation and any history of abuse.

LinkedIn has numerous workstreams that address misinformation, particularly during crisis situations like COVID-19. During such a crisis, LinkedIn:

- proactively provides members with trustworthy information through news storylines created by our in-house team of global news editors;
- showed banners that took members to this trustworthy information when our members searched for COVID-related terms.
- removes misinformation related to COVID and updates the applicable policies as needed;
- has multiple internal teams who ensure that both ads customers and state-sponsored actors do not exploit the crisis.

LinkedIn's in-house editorial team provides members with trustworthy content regarding global events, including for example Russia's war against Ukraine. LinkedIn has an internal team of hundreds of content reviewers located all over the world providing 24/7 coverage and includes specialists in a number of languages.

**Outcome 1b: Users will be informed about the types of behaviours and types of content that will be prohibited and/or managed by Signatories under this Code.**

Users can find information about the types of behaviours and content that will be prohibited and/or managed as follows:

- **Microsoft Advertising:** [Microsoft Advertising policies](#)
- **Microsoft Start:** [Microsoft Services Agreement, Community Guidelines](#)

- **LinkedIn:** [User Agreement](#), [Professional Community Policies](#)

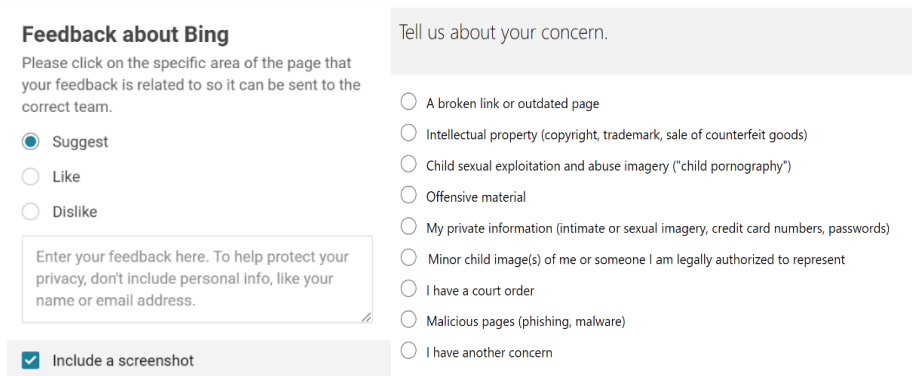
Outcome 1c: Users can report content and behaviours to Signatories that violate their policies under 5.10 through publicly available and accessible reporting tools.

In addition to the guidelines contained within the respective user agreements, **Bing Search**, **Microsoft Start**, **Microsoft Advertising** and **LinkedIn** have reporting mechanisms where users are able to flag problematic content.

### Bing Search

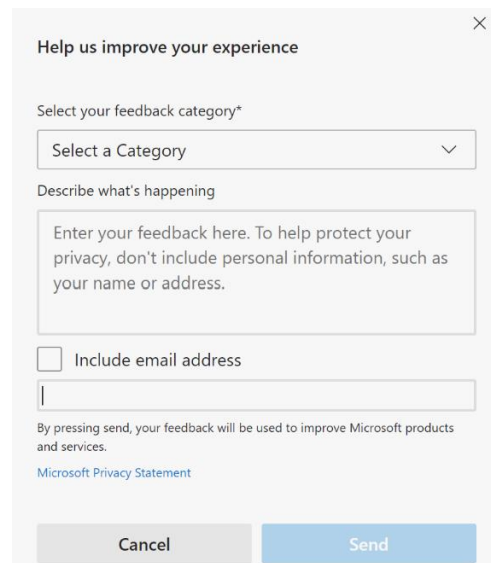
**Bing Search's** "Feedback" tool, which is accessible on the lower right corner on a search results page, allows users to provide feedback on search results (including a screenshot of the results page) to Bing Search.

Depending on the nature of the feedback, Bing Search may take appropriate action, such as undertaking defensive search interventions, delisting a website, or removing autosuggest terms, depending on the nature of the feedback.



### Microsoft Start

**Microsoft Start** includes a feedback feature at the bottom of all pages (landing page and each article, see below), with Content Quality as one of the options in the drop-down menu. This feedback feature is also included in the Settings menu.



## Microsoft Advertising

**Microsoft Advertising** enables users to report ads which may be in violation of its policies (e.g., ads that may contain malvertising, disallowed content, relevancy concerns, or sensitive content) through its [low quality ad submission and escalation form](#) (as shown below). Users of Bing Search and Microsoft Start can also report ads via the respective feedback functions on those services.

### Low quality ad submission & escalation

Have you found an occurrence of a low quality ad on Microsoft Bing? Let us know! A low quality ad is one where the ad contains one or more of the following attributes:

- **Malvertising:** Describes advertising practices that have malicious intent to cause harm or defraud a user.
- **Disallowed content:** Refers to issues with landing page content/products/services that are not allowed in ads.
- **Relevancy concerns:** Poor relevancy can occur when an advertiser associates a keyword to a landing page or ad copy where no logical association exists (for example, a query for "Facebook" yields ad copy and a landing page for golf supplies).

Fill out the form below to submit an ad quality escalation.

\*Required

Please enter your search query term\*

Please enter the ad link (found on the Bing results page)\*

This is not the display URL found in the ad. To copy the link:

1. Right click the ad site
2. Select Copy shortcut
3. Paste into the box below

Email\*

Confirm email address\*

Country/Region\*

#### Ad attributes or issues

Please check the relevance, content or malvertising issues that are relevant to the ad(s) being escalated:

##### Disallowed content

- The ad's landing page has disallowed content  The ad's landing page is promoting disallowed products or services  
 Other disallowed content issue (explain in Comments section below)

##### Relevance

- The ad is not relevant to what I was looking for  The landing page is not relevant to what I was looking for  
 Ad copy does not make sense  The display URL I saw in the ad does not match the landing page  
 Other relevance issue (explain in Comments section below)

##### Page or site quality

- High percentage ads or links on the landing page  Low value, sparse or limited content across the site  
 This site redirects me to a completely unrelated location/domain  
 Other page or site quality issue (explain in Comments section below)

##### Personally identifiable information (PII)

- Site asks me for personal information that I wouldn't expect to have to share  Phishing

##### Malicious

- This site gave me a virus, or seems to host malware or spyware  This site/business seems deceptive or fraudulent  
 Other malicious issue (explain in Comments section below)

##### Landing page navigation

- Site changes browser preferences without my consent  
 Site spawns multiple pop ups or pop ups that prevent me from leaving the site  Landing page does not load  
 I am getting a 'product not available' message  
 Other landing page navigation issue (explain in Comments section below)

##### Sensitive content

- Ad exploits a sensitive tragedy, disaster, death or high profile news event, or is considered inappropriate given current events

Comments

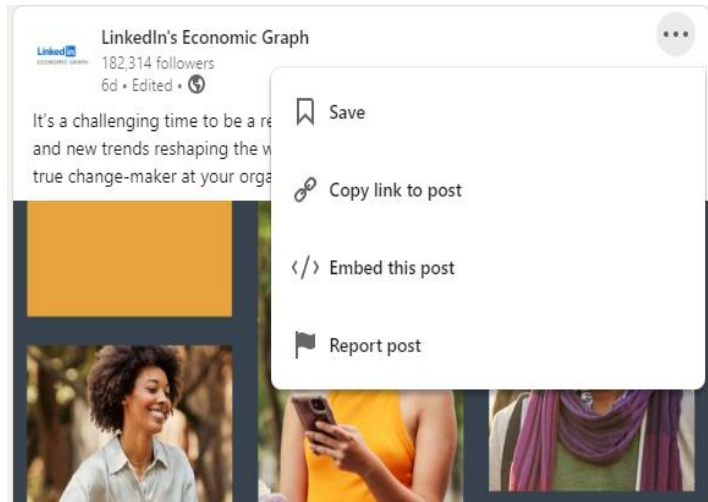
- I would like information, tips and offers about Microsoft Advertising. [Privacy Statement](#)

 I'm not a robot 

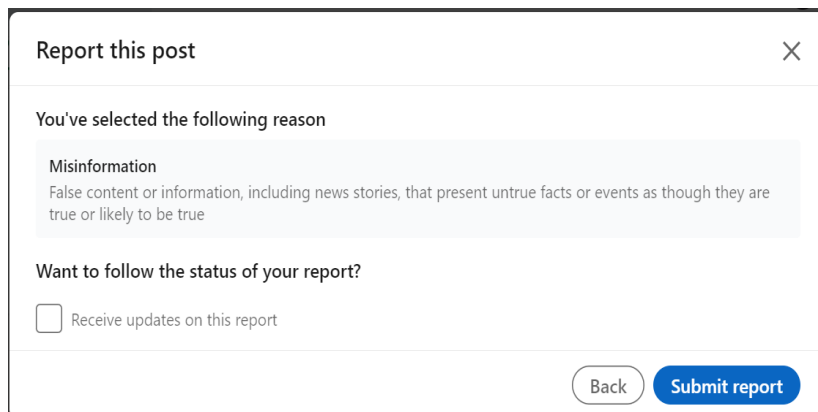
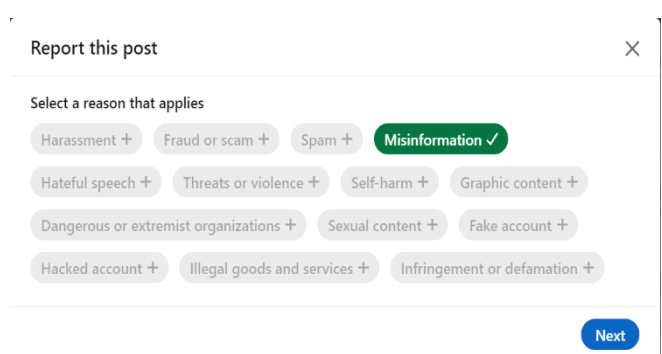
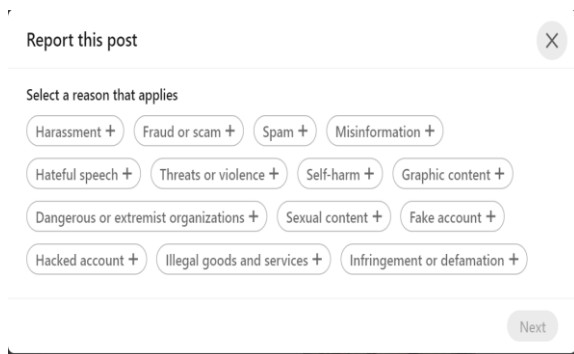
Submit

## LinkedIn

If **LinkedIn's** members locate content they believe violates our **Professional Community Policies**, we encourage them to report it using the in-product reporting mechanism represented by the three dots in the upper right hand corner of a post on LinkedIn:



Misinformation is specifically called out as one of the reporting options.



LinkedIn is in the process of rolling out an updated version of its reporting flow. The above screenshots reflect that new flow, which is currently available to members located in Australia for certain types of content. However, misinformation also was specifically called out as a potential reporting reason under the previous version of the flow which was in place in 2022.

Reported content is generally reviewed by trained content reviewers. In addition, LinkedIn uses automation to flag potential violations including disclosure of private information, spam and malicious pages, and illegal materials content to our content moderation teams. If





reported or flagged content is found to violate the Professional Community Policies, it will be removed from the platform.

When members use the above reporting process and choose to receive updates, LinkedIn communicates by email with the reporting member to confirm receipt of reports and provide updates about subsequent decisions. Members also generally receive notice in the event their content is removed from LinkedIn.

If members wish to appeal LinkedIn’s decisions, they can request a second review and provide the reasons they believe LinkedIn’s decision was not correct. To begin that appeal process, members can log into their account and follow the onscreen messaging or reply to the message they received notifying them of the content removal.

[Outcome 1d: Users will be able to access general information about Signatories actions in response to reports made under 5.11.](#)

**Bing Search, Microsoft Start, Microsoft Advertising**

In addition to the sources detailed above, Microsoft regularly publishes information about the detection and removal of content that violates our policies or is subject to removal under local legal obligations in the Digital Trust section of our [Reports Hub](#).

**LinkedIn**

The [LinkedIn Community Report](#) describes actions we take on content that violates our Professional Community Policies and User Agreement. It is published twice per year and covers the global detection of fake accounts, spam and scams, content violations and copyright infringements.

**LinkedIn Community Report: global actions taken on content that violated Professional Community Policies and User Agreement, January 2019 – December 2022**

		2019 Jan-Jun	2019 Jul-Dec	2020 Jan-Jun	2020 Jul-Dec	2021 Jan-Jun	2021 Jul-Dec	2022 Jan-Jun	2022 Jul-Dec
<b>Global</b>	<b>Fake Accounts</b> Stopped at registration	19.5m	7.8m	33.7m	11.6m	11.6m	11.9m	16.4m	44.7m
	Restricted proactively	2m	3.4m	3.1m	3.0m	3.7m	4.4m	5.4m	13.2m
	Restricted after report	67.4k	85.6k	103.1k	111k	85.7k	127k	190k	201k
	<b>Content Violation</b> Misinformation*			22.8k	110.7k	147.5k	207.5k	172.4k	138k

		2019 Jan-Jun	2019 Jul-Dec	2020 Jan-Jun	2020 Jul-Dec	2021 Jan-Jun	2021 Jul-Dec	2022 Jan-Jun	2022 Jul-Dec
<b>Australia#</b>	<b>Fake Accounts</b> Stopped at registration					54,883	45,983	81,533	149,591
	Restricted proactively					64,642	39,179	63,317	112,809
	Restricted after report					1,281	1,448	1,755	2,023
	<b>Content Violation</b> Misinformation*					2,149	6,007	3,946	1,656
	Misinformation content removals that were appealed by the content author						219	151	79
	The number of appeals that were granted						3	3	3

\*Misinformation not reported as a separate category prior to 2020. Other content violation categories reported are harassment or abusive, adult, hateful or derogatory, violent or graphic, child exploitation.

#Australian data not reported separately prior to 2021.

## Objective 2: Disrupt advertising and monetisation incentives for Disinformation.

Outcome 2: Advertising and/or monetisation incentives for Disinformation are reduced.

Microsoft strives to provide our customers with a positive online experience free from deceptive advertisements. Microsoft is working across our services to achieve this goal through policies and enforcement processes aimed at ensuring that the advertising and content served is clear, truthful, and accurate.

### Microsoft Advertising

In December 2022, **Microsoft Advertising** rolled out revised network-wide policies to avoid the publishing and carriage of harmful disinformation and the placement of advertising next to disinformation content. Such policies prohibit ads or sites that contain or lead to disinformation. To enforce this policy, we may use a combination of internal signals and trusted third-party data or information sources to reject, block, or take down ads or sites that



contain disinformation or send traffic to pages containing disinformation. We may block at the domain level landing pages or sites that violate this policy.

Microsoft Advertising works with selected, trustworthy publishing partners and requires these partners to abide by strict brand safety-oriented policies to avoid providing revenue streams to websites engaging in misleading, deceptive, harmful, or insensitive behaviours.

Microsoft Advertising's policies with respect to these publishers include a comprehensive list of prohibited content that ads cannot serve against. Prohibited content includes, but is not limited to:

- disinformation;
- sensitive content (e.g., extreme, aggressive, or misleading interpretations of news, events, or individuals);
- unmoderated user-generated content; and
- unsavoury content (such as content disparaging individuals or organisations).

Publishers are required to maintain a list of prohibited terms and provide us with information on their content management practices where applicable. In addition to content requirements, publishers are required to abide by restrictions against engaging in business practices that are harmful to users (e.g., distributing malware).

Microsoft Advertising reviews publisher properties and domains for policy compliance, including compliance with restrictions on prohibited content. In this review, Microsoft Advertising also considers feedback from its advertisers to help ensure a safe environment for the delivery of their advertisements and maintains a review process to investigate related advertiser complaints.

Publishers are promptly notified of properties or domains that violate Microsoft Advertising's policies; such properties and domains are not approved by Microsoft for live ad traffic. If a property or domain is already live, and later found in violation of Microsoft Advertising's policies, it is removed from the network until the publisher remedies the issue.

### **LinkedIn**

**LinkedIn** prohibits misinformation and disinformation on its platform, whether in the form of organic content or in the form of advertising content.

LinkedIn's [Professional Community Policies](#), which apply to all content on LinkedIn's platform, expressly prohibit false and misleading content, including misinformation and disinformation. LinkedIn provides additional specific examples of false and misleading content that violates its policy via a [Help Center article on False or Misleading Content](#).

LinkedIn's [Advertising Policies](#) incorporate the above provision, and similarly prohibit misinformation and disinformation. In addition, LinkedIn's Advertising Policies also prohibit

fraudulent and deceptive ads, and require that any claims made in an ad have factual support.

Of note, unlike some other platforms, LinkedIn does not allow members to monetise or run ads against their content, nor does it offer an ad revenue share program. Thus, members publishing disinformation on LinkedIn are not able to monetise that disinformation or collect advertising revenue via LinkedIn.

LinkedIn members may also report ads that they believe violate LinkedIn's advertising policies and, when members report ads, LinkedIn's advertising review team reviews them. To report an ad, members can click on the three-dot icon in the upper right-hand corner of every ad and select the "Hide or report this ad" option.

**Objective 3: Work to ensure the security and integrity of services and products delivered by Digital platforms.**

**Outcome 3: The risk that inauthentic user behaviours undermine the integrity and security of services and products is reduced.**

In addition to the actions detailed in Objective 1 (Outcomes 1a, 1b and 1c), **Bing Search**, **Microsoft Advertising**, and **LinkedIn** reduce the risk of inauthentic user behaviours through the measures detailed below.

### **Bing Search**

The "Abuse and Examples of Things to Avoid" section of the Bing Webmaster Guidelines details the policies intended to maintain the integrity of Bing Search. Bing's general spam policies prohibit certain practices intended to manipulate or deceive the Bing search algorithms, including those employed by malicious actors in the spread of disinformation.

Bing may take action on websites employing spam tactics or that otherwise violate the Webmaster Guidelines, including by applying ranking penalties (such as demoting a website or delisting a website from the index). However, it is important to clarify that in search it is not feasible to distinguish between spam tactics employed by malicious actors specifically for the purpose of spreading disinformation and other types of spam.

In addition to enforcing its spam policies, Bing takes actions to promote high authority, high quality content and thereby reduce the impact of disinformation appearing in Bing search results. Among other initiatives, this includes:

- continued improvement of its ranking algorithms to ensure that the most authoritative, relevant content is returned at the top of search results;
- regular review and actioning of disinformation threat intelligence;
- partnership with fact-checking and media literacy organisations;
- contributing to and supporting the research community; and



- implementation and enforcement of clear policies concerning the use of manipulative tactics on Bing Search.

Although the Bing search algorithms endeavour to prioritise relevance, quality, and credibility in all scenarios, in some cases Bing identifies a threat that undermines the efficacy of its algorithms. When this happens, Bing employs “defensive search” strategies and interventions to counteract threats in accordance with its trustworthy search principles to help protect Bing users from being misled by untrustworthy search results and/or inadvertently being exposed to unexpected harmful or offensive content.

In addition to defensive search, Bing Search regularly monitors for violations of its Webmaster Guidelines, including attempts to manipulate the Bing search algorithms through prohibited practices such as cloaking, link spamming, keyword stuffing, and phishing.

### **Microsoft Advertising**

**Microsoft Advertising** employs a robust filtration system to detect bot traffic.

- This system uses various algorithms to automatically detect and neutralise invalid or malicious online traffic which may arise from or result in click fraud, phishing, malware, or account compromise.
- The system is supported by several teams of security engineers, support agents, and traffic quality professionals who continually develop and improve monitoring and filtration.
- Support teams work closely with advertisers to review complaints around suspicious online activity and across internal teams to verify data accuracy and integrity.

### **LinkedIn**

LinkedIn’s professional focus shapes the type of content we see on platform. People tend to say things differently when their colleagues and employer are watching. Accordingly, our members don’t tend to use LinkedIn to engage in the mass dissemination of misinformation, and bad actors generally need to create fake accounts to peddle misinformation.

To ensure their content reaches a large audience, bad actors need to either connect with real members or post content that real members will like— both of which are hard to achieve on LinkedIn given our professional focus. The mass dissemination of false information, as well as artificial traffic and engagement, therefore, requires the mass creation of fake accounts, which we have various defences to prevent and limit.

To respond to the ever-changing threat landscape, our team continually invests in new technologies for combating inauthentic behaviour on the platform. We are investing in artificial intelligence technologies such as advanced network algorithms that detect communities of fake accounts through similarities in their content and behaviour, computer vision and natural language processing algorithms for detecting AI-generated elements in fake profiles, anomaly detection of risky behaviours, and deep learning models for detecting sequences of activity that are associated with abusive automation.

LinkedIn also acts vigilantly to maintain the integrity of all accounts and to ward off bot and

false account activity (including “deep fakes”). LinkedIn enforces the policies in its [User Agreement](#) prohibiting the use of “bots or other automated methods to access the Services, add or download contacts, send or redirect messages” through:

- having a dedicated Anti-Abuse team to create the tools to enforce this prohibition;
- using automated systems detect and block automated activity;
- imposing hard limits on certain categories of activity commonly engaged in by bad actors;
- detecting whether members have installed known prohibited automation software;
- conducting manual investigation and restriction of accounts engaged in automated activity;
- partnering with the broader Microsoft organisation to develop technological solutions for protecting content provenance and identification of deep fakes;
- investing in and using AI to detect coordinated inauthentic activity and communities of fake accounts through similarities in their content and behaviour;
- using third party fact checking sites during the human content review process when suspected deepfakes are flagged or found on the platform; and
- “hashing” known instances of deepfake content, which can be used to find copies of the same content on our platform.

#### Objective 4: Empower consumers to make better informed choices of digital content.

Outcome 4: Users are enabled to make more informed choices about the source of news and factual content accessed via digital platforms and are better equipped to identify Misinformation.

Microsoft is committed to helping our customers make informed decisions about content. This includes providing our customers with tools to help them evaluate the trustworthiness of that content.

Microsoft is working both internally and with third parties to provide new tools and implement new technologies across our services to assist our customers in identifying trustworthy, relevant, authentic, and diverse content, including in news, search results, and user-generated material.

#### **Bing Search**

**Bing Search** offers a number of tools to help users understand the context and trustworthiness of search results. Even in circumstances where a user is expressly seeking low authority content (or if there is a data void so little to no high authority content exists for a query), Bing Search provides tools to users that can help improve their digital literacy and avoid harms resulting from engaging with misleading or inaccurate content. For example:

- Bing Search often includes answers or public service announcements at the top of search results pointing users to high authority information on a searched topic or

warnings on particular URLs known to contain harmful information (such as unaccredited online pharmacies and sites containing malware).

- Where circumstances warrant (such as public health crises or major elections), Bing Search may provide information hubs for users to easily access a centralised repository of high authority information.

### *NewsGuard*

Microsoft also partners with NewsGuard to help users evaluate the quality of the news they encounter online. NewsGuard launched in Australia in March 2023 and is currently also available in US, UK, Canada, France, Italy, and Germany.

- NewsGuard has created trust ratings for more than 7,500 news and information sites, which are compiled into a “Nutrition Label” and corresponding Red/Green Reliability Rating to help users understand the reliability of news sources.
- Microsoft offers NewsGuard as a free plug-in for the Microsoft Edge web browser (it is also available for other browsers including Chrome and Firefox), and users of the Edge mobile application on both iOS and Android can enable NewsGuard ratings in their app settings.
- For users with the NewsGuard plug-in, Bing Search results include NewsGuard Reliability ratings that lead to a pop-up screen with more site information.

As it was launched after the reporting period, we will include more information on the NewsGuard plug-in’s adoption in Australia in future reports.

### *Search Coach*

In June 2022, Microsoft introduced [Search Coach](#) to help students form effective queries when searching for reliable resources online using Bing or other search engines.

Search Coach filters include:

- **Domains:** Selecting Domains reveals descriptions of common top-level domains, including information about how that domain reflects on the reliability of a site and things to look out for.
- **Filetypes:** Retrieve only PDF articles, only PowerPoints, only Docs.
- **Date Range:** Filter for items appearing today, last week, etc., or set a date range
- **Operators:** To specify exact matches, articles that do *not* mention a term, and others.
- **Fact Checking:** a set of objective fact check sites that can appear as a fifth filter button.
- **Custom filter:** Educator-created lists of subdomains for students to search over.

### **Microsoft Start**

In response to the invasion of Ukraine, **Microsoft Start** added a dedicated “War in Ukraine” news section in March 2022, to enable users to easily access trustworthy news content on the issue.



Microsoft Start clearly labels advertising to enable users to readily distinguish this from other content.

## **LinkedIn**

As the world around us changes, **LinkedIn** continues to evolve and adapt our systems and practices for combating misinformation and other inauthentic behaviour on our platform, including to respond to the unique challenges presented by world events.

In addition to broader measures, LinkedIn has taken steps to tackle disinformation in connection with unfolding world events. In response to the COVID-19 pandemic, LinkedIn editors created and promoted trusted content. LinkedIn introduced the following measures:

- Promote content from most credible organisations and experts, such as the World Health Organization.
- During the early years of the pandemic, redirected any member that undertook a simple search of the term “coronavirus” to a link “Know the facts about coronavirus”, which appears first in the list of search results. By clicking on this link, members are directed to LinkedIn’s own official page on the coronavirus with information and broadcasts from verified sources, primarily from the World Health Organization. The storylines on this page were available in 8 languages across 54 countries, including Australia.
- Launched a ‘Special Report: Coronavirus’ box above ‘Today’s News and Views’ with story lines relevant to COVID-19 and including updates from the World Health Organization and Centers for Disease Control and Prevention.

LinkedIn’s internal, global team of global experienced news editors also proactively provide members with curated news about current events from trusted sources in a number of languages.

- LinkedIn’s team of editors cover the most recent developments of Russia’s invasion of Ukraine, ranging from the economic impact to major military events that are taking place.

LinkedIn does not prioritise any news sources in our feed, but in crisis situations, (e.g., COVID-19 or the war in Ukraine), we will use search banners to point members to reputable sources of information (e.g., when members searched for COVID, we pointed members to “trusted storylines” where we provided trustworthy information about those topics, including links to global health organisations).

As mentioned above, Microsoft has partnered with NewsGuard to provide a free plug-in for the Microsoft Edge web browser (also available for other browsers). LinkedIn members are also able to benefit from NewsGuard via this plug in which enables LinkedIn members to benefit from NewsGuard’s reliability rating, where available, when browsing news posts from news and information sites rated by NewsGuard.



**In October 2022, LinkedIn announced the introduction of a new “About this profile” feature.**

- This feature has been rolled out worldwide, including in Australia.
- The feature will show users when a profile was created and last updated, along with whether the member has verified a phone number and/or work email associated with their account.
- This feature is part of our ongoing commitment to help members make more informed decisions about members with whom they interact, and enhancing our automated systems that keep inauthentic profiles and activity off our platform, and empowering members with additional signals about the authenticity of accounts.

**Other contributions and measures**

Globally, Microsoft also has a number of programs to proactively combat disinformation on our services and empower users.

Microsoft expects that methods for generating synthetic media, or “deep fakes”, which are photos, videos or audio files manipulated by AI in hard-to-detect ways, will continue to grow in sophistication.

- As all AI detection methods have rates of failure, platforms must understand and be ready to respond to deep fakes that slip through detection methods.
- In the longer term, there will be a need for stronger methods for maintaining and certifying the authenticity of news articles and other media.

There are few tools today to help assure readers that the media they are seeing online came from a trusted source and that it was not altered.

Microsoft is devoting research resources to find innovative solutions to this problem, including through measures outlined in detail in our 2022 Transparency Report, such as:

- creating [Video Authenticator](#) , a tool to address deep fakes by providing a confidence score that a still photo or video was artificially manipulated;
- developing [Project Origin](#), a technology to help certify the source of the content, like a watermark, to give publishers and consumers a tool to identify when media has been altered from the original source; and
- being a founding member of the [Coalition for Content Provenance and Authenticity \(C2PA\)](#), which aims to address the prevalence of disinformation, misinformation, and online content fraud through developing technical standards for certifying the source and history or provenance of media content.

Please also see response to Objective 6

**In March 2023, Microsoft and Truepic announced the pilot in Ukraine of “Project Providence.”**

The project is the world’s first interoperable system using Truepic’s authenticating camera SDK and the Microsoft Azure cloud platform to maintain the provenance or origin of images captured, from storage to display. This enables users to verify images as authentic and transparently display their time, date, location, and source to viewers. With this technology, modifications to the images can be detected and the authentic source of images can be proven.

The platform is being used first by a group of documenters associated with the Ukrainian non-government organisation, Anti-Corruption Headquarters. The team in Ukraine is documenting damage to cultural heritage and national infrastructure for accountability, advocacy, and reconstruction efforts. The Project Providence platform leverages the Coalition for Content Provenance and Authenticity (C2PA) open standard to allow end-to-end interoperability between the capture of documentation, storage, and display.

Today, manipulated online content is becoming more sophisticated. This pilot is a key step in Microsoft’s efforts to create technologies that empower people to find, consume and share authoritative and trusted information. Having proof-of-concept that we can certify the provenance of an image – the origin, authenticity, and history – is a powerful tool in that effort. This is one way, through the Microsoft Democracy Forward initiative, we are supporting healthy information ecosystems in Ukraine and around the world.

**Objective 5: Improve public awareness of the source of Political Advertising carried on digital platforms.**

**Outcome 5: Users are better informed about the source of Political Advertising.**

**Microsoft Advertising**

Under our Advertising Policies, **Microsoft Advertising** prohibits political advertising. This includes ads for election-related content, political candidates, parties, ballot measures, and political fundraising globally; similarly, ads aimed at fundraising for political candidates, parties, political action committees (PACs), and ballot measures also are barred.

All Microsoft and third-party services that rely on Microsoft Advertising to serve advertisements on their platforms benefit from these robust, and robustly enforced, set of policies.

Specifically, Microsoft Advertising employs dedicated operational support and engineering resources to enforce restrictions on political advertising using a combination of proactive and reactive mechanisms.



- On the proactive side, Microsoft Advertising has implemented several processes designed to block political ads from showing across its advertising network, including restrictions on certain terms and from certain domains.
- On the reactive side, if Microsoft Advertising becomes aware that an ad suspected of violating its policies is being served to our publishers—for instance, because someone has flagged that ad to our customer support team—the offending ad is promptly reviewed and, if it violates our policies, taken down.

Microsoft Advertising’s policies also prohibit certain types of advertisements that might be considered issue based. More specifically, “advertising that exploits political agendas, sensitive political issues or uses ‘hot button’ political issues or names of prominent politicians is not allowed regardless of whether the advertiser has a political agenda,” and “advertising that exploits sensitive political or religious issues for commercial gain or promote extreme political or extreme religious agendas or any known associations with hate, criminal or terrorist activities” are also prohibited.

**LinkedIn**

LinkedIn does not accept political advertising. LinkedIn’s [Advertising Policies](#) globally prohibit political ads which:

- advocate for or against a particular candidate, party or ballot proposition or are otherwise intended to influence an election outcome;
- fundraise for or by political candidates, parties, ballot propositions or PACs or similar organisations; and
- exploit a sensitive political issue even if the advertiser has no explicit political agenda.

All ads are subject to review for adherence to policy before being approved to run. LinkedIn has also introduced features making it simple for members to [report advertisements](#) that violate LinkedIn’s policies; LinkedIn reviews such reports and removes offending advertisements from its platform.

**Objective 6: Strengthen public understanding of Disinformation and Misinformation through support of strategic research.**

**Outcome 6: Signatories support the efforts of independent researchers to improve public understanding of Disinformation and Misinformation.**

Microsoft is working at a company-wide level to ensure that the research community has the tools and resources it needs to play its crucial part in helping to combat disinformation. A non-exhaustive list of Microsoft’s ongoing collaborations with the broader research community in this space include:

<a href="#">Microsoft SearchData on COVID-19 Queries and Misinformation Research Support</a>	In 2020, Bing Search shared a <a href="#">search dataset</a> for Coronavirus Intent comprised of queries from all over the world that had an intent related to the Coronavirus or Covid-19 (e.g., searches for “Coronavirus updates Seattle”)
--	---

	<p>or “Shelter in place”) for use by researchers and the public on <a href="#">GitHub</a>.</p> <p>This data, which is divisible by country, is particularly relevant to misinformation research on public health issues and the COVID-19 pandemic, as it provides insights into how users sought information related to the coronavirus during the pandemic.</p> <p>The dataset was also posted to <a href="#">Azure Open datasets for Machine Learning</a>, <a href="#">Tensorflow.org</a> and <a href="#">Kaggle</a>. This dataset has already been used by the disinformation research community. For example, Researchers at Aalborg University used the dataset as part of their research paper “<a href="#">Does Vinegar Kill Coronavirus? - Using Search Log Analysis to Estimate the Extent of COVID-19-Related Misinformation Searching Behaviour in the United States</a>”. The Aalborg University study used Bing search log analysis to investigate the extent and characteristics of misinformation seeking behaviour in the US.</p>
<p>Partnership with Princeton University and Carnegie Endowment for International Peace</p>	<p>Microsoft is partnering with Princeton University and the Carnegie Endowment for International Peace to fund and provide data to the Institute for Research on the Information Environment (IRIE), an international resource to study information ecosystems that can spur evidence-based policy solutions.</p>
<p><a href="#">Technology   Academics   Policy (TAP)</a></p>	<p>TAP is a forum for leading academics to share articles, ideas and research that focus on the impact of technological change with each other and the broader online community.</p> <p>Microsoft provides administrative and financial support.</p>
<p><a href="#">Oxford Technology and Elections Commission (OxTEC)</a>, Oxford Internet Institute</p>	<p>Microsoft supports OxTEC to research how democracies can integrate democratic norms and practices into the use of information technologies, social media, and big data during campaigns, with the goal of protecting the integrity of elections.</p>
<p><a href="#">Trust Project</a></p>	<p>Microsoft Start, then Bing News, joined the Trust Project in 2017. The consortium led through Santa Clara University’s Markkula Center for Applied Ethics, to develop a standardised technical language for platforms to learn more from news sites about quality and expertise behind journalists’ work.</p>

	<p>This Project includes organisations such as the Washington Post, the Economist, and the CBC. It does not yet list any Australian partners.</p> <p>The Trust Project is the first to give search engines and social media platforms the consistent technical standards they need to surface reliable, relevant, and honest news. Bing Search uses the Trust Indicators in display and behind the scenes in some markets.</p>
Microsoft Research Lab	<p>Microsoft Research dedicates significant resources to supporting, promoting, and developing research on emerging issues including responsible AI, safe design, search and information retrieval, and algorithms. Microsoft Research teams regularly utilise Bing Search datasets as part of important research efforts, including those focused on misinformation and disinformation.</p> <p>For example, Microsoft Research is currently working on research related to medical hoaxes and another project concerning improvements to autosuggest with respect to news articles.</p> <p>Microsoft Research and the AI for Good team have also used Bing data in ongoing studies of how Russian propaganda is consumed and how new propaganda websites appear. Bing will provide additional updates as the research is made public.</p> <p>Microsoft Research maintains a public portal of codes, APIs, software development kits, and datasets that are available to the <a href="#">Research Community at Researcher tools: code &amp; datasets – Microsoft Research</a>. Microsoft Research also created <a href="#">Microsoft Research Open Data (msropendata.com)</a>, a data repository of datasets that researchers at Microsoft have created and published in conjunction with their research (including datasets derived from Bing Search). These public research tools can be accessed by researchers and downloaded instantaneously without formal applications or login credentials.</p>
<u>Partnership on AI</u>	<p>Microsoft is a partner in Partnership on AI which works to better understand and address the emerging threat posed by the use of AI tools to develop malicious synthetic media (i.e., deep fakes).</p>
<u>MS MARCO</u>	<p>Bing Search makes information available to the research community to improve search results by making data sets</p>

	<p>like its MS MARCO publicly available. Bing Search provides researchers and the public with access to MS MARCO, a collection of datasets focused on deep learning in search that are derived from Bing queries and related data. Research organisations can gain access to the MS MARCO datasets instantaneously via the MS MARCO homepage. The MS MARCO dataset has been cited in over 1400 research papers since its release and has been used for a range of research issues, including in relation to misinformation and disinformation. Because the dataset is provided open source, the extent to which it has been used for disinformation related research purposes cannot easily be ascertained. However, the dataset has been cited in various academic papers concerning misinformation and disinformation, including:</p> <ul style="list-style-type: none"> <li>• <a href="#">Generating Fact Checking Briefs</a> - Facebook AI Research, University College London LORIA, and University of Cambridge</li> <li>• <a href="#">H2oloo at TREC 2020: When all you got is a hammer... Deep Learning, Health Misinformation, and Precision Medicine</a> - University of Waterloo</li> <li>• <a href="#">Detecting fake news using Natural Language Processing</a> – Politecnico di Torino</li> </ul>
Other publicly shared datasets	<p>Bing Search also offers use of <a href="#">Bing APIs</a> to the public, which include services such as Bing Image Search, Bing News Search, Bing Web Search. Bing Search provides free access to these APIs for up to 1,000 transactions per month, which may be leveraged by the research community. Bing News Search API, for example, has been used in connection with research on disinformation in a 2022 research paper, "<a href="#">A Proposal to Find Fake News and Detecting Political Bias of News Articles</a>" published in <i>Advances in Data and Information Sciences</i>, a collection of peer-reviewed research papers presented at the 3rd International Conference on Data and Information Sciences.</p> <p>Given the open nature of the Bing Search index and public nature of search results, researchers can use Bing to run specific queries and analyse results (unlike social media which may require private accounts or connections between users to access certain materials).</p>

### *Democracy Forward Program*

Microsoft believes technology companies have a responsibility to help protect democratic processes and institutions globally. Though threats to democracy have always existed, the tactics of adversaries are constantly evolving. Microsoft is protecting open and secure democratic processes by providing services and technology to secure critical institutions, protect electoral processes from cyberattacks, and build public trust in voting procedures.

Microsoft's Democracy Forward Program is an innovative effort to protect democratic institutions and processes from hacking, to explore technological solutions to protect electoral processes, and to defend against disinformation.

- Microsoft works closely with our elections-related customers to provide security guidance and tools to improve their cyber-resilience and protect the integrity of the electoral process.
- In 2022, Microsoft supported the International Foundation for Electoral Systems (IFES) to strengthen the cybersecurity practices of investigative journalists who are reporting on abuse of state resources in elections. We also partner with the National Democratic Institute (NDI) to strengthen the cybersecurity support infrastructure for political parties and campaigns internationally.
- In March 2023, Microsoft, USAID and Internews announced a new public-private partnership to develop a Media Viability Accelerator to help independent media outlets around the world become more financially sustainable through access to market insights and business solutions. The new web-based platform will pool data from media organisations globally to enable independent newsrooms to discover what works for others and apply those learnings to their own business. Once launched, independent news organisations in more than 100 countries will be able to use the Media Viability Accelerator to support their mission to provide the public with reliable, trustworthy information.

### Objective 7: Signatories publicise the measures they take to combat Disinformation and Misinformation.

Outcome 7: The public can access information about the measures Signatories have taken to combat Disinformation and Misinformation.

Our reporting under this code is available on the [Microsoft Australia News Centre](#) and on [DIGI's website](#).

Microsoft also releases other information about our initiatives globally to combat disinformation:

<a href="#"><u>Microsoft On the Issues</u></a>	Blog contains announcements on technology policy issues, including disinformation. For example, our response to the invasion of Ukraine, COVID-19, video authenticator technology, release of digital trust reports, are all posted on the blog
<a href="#"><u>Microsoft Reports Hub</u></a>	Transparency reports include Digital Safety Content Report and Government Requests for Content Removal Report.
<a href="#"><u>Microsoft Digital Defense Report</u></a>	Report encompasses learnings from security experts, practitioners, and defenders at Microsoft to empower people everywhere to defend against cyberthreats. Includes dedicated section on disinformation.
<a href="#"><u>LinkedIn Transparency Center</u></a>	<a href="#"><u>Community Report</u></a> <a href="#"><u>Government Requests Report</u></a>
<a href="#"><u>LinkedIn Blog</u></a>	Blog contains information on actions to combat disinformation, including <a href="#"><u>New LinkedIn profile features help verify identity, detect and remove fake accounts, boost authenticity</u></a> , <a href="#"><u>How We're Protecting Members From Fake Profiles</u></a> , <a href="#"><u>Automated Fake Account Detection</u></a> , and <a href="#"><u>An Update on How We Keep Members Safe</u></a>

## Conclusion

Microsoft is committed to playing our part in supporting a trustworthy information ecosystem through application of our policies, our own research and innovation in new technologies, and collaboration with partners, academia, and our users. This report details some of the initiatives Bing Search, Microsoft Start, Microsoft Advertising and LinkedIn are taking to reduce and disrupt the propagation of disinformation and misinformation, as well as the efforts the company is taking to contribute to the goals and commitments of the Australian Voluntary Code of Practice on Disinformation and Misinformation.