

EU CODE OF PRACTICE ON DISINFORMATION 2022

# Subscription Document for Twitch Interactive, Inc.

**Name of the Signatory**

*Twitch Interactive, Inc.*

**About the Signatory****Overview**

Twitch is a service for sharing live, interactive long-form video content; streamers on Twitch primarily stream themselves playing video games, but a small segment of streamers broadcast in a number of different categories of content (e.g., cooking, talk shows, body art, and more). Streamers typically build a community over time by streaming for multi-hour sessions over a sustained period. Some streamers with large audiences eventually stream on Twitch as a full time job, although even small or mid-sized streamers have the option to monetize so long as they meet our minimum requirements. All streamers and viewers must remain in compliance with our policies at all times.

**Approach to Safety**

At Twitch we take a layered approach to safety - one that combines the efforts of both Twitch (through tooling and staffing) and members of the community (streamers and viewers), working together. It starts with our Community Guidelines, which balance user expression with community safety, and set expectations for the behaviour we want on Twitch. Creators are expected to uphold these service-wide standards in their channels, and are invited to raise the bar if they choose. We provide creators with tools to set, communicate and enforce the standards of behaviour in their channel. We also provide viewer-level controls that enable viewers to control the content they see. At the same time, Twitch applies various technologies to proactively detect and remove certain kinds of harmful content before users ever encounter it. Finally, we empower users to report harmful or inappropriate behaviour to Twitch. These reports are reviewed and acted on by a team of skilled and trained professionals who can apply service-wide enforcement actions.

**Approach to Disinformation**

In order to reduce harm to our community and the public without undermining our streamers' open dialogue with their communities, we prohibit harmful misinformation superspreaders who persistently share misinformation on or off of Twitch. We seek to remove users whose online presence is dedicated to (1) persistently sharing (2) widely disproven and broadly shared (3) harmful misinformation topics.

This policy is focused on Twitch users who persistently share harmful misinformation. It will not be applied to users based upon individual statements or discussions that occur on a channel. We evaluate whether a user violates the policy by assessing both their on-platform behaviour as well as their off-platform behaviour. In addition to this policy, we also cover misinformation that targets protected groups under our [Hateful Conduct & Harassment Policy](#)

Service name	Description of the service
Twitch	Please see Overview section above

II Scrutiny of Ad Placements		
List of adopted commitments and measures		Qualitative reporting elements and service level indicators
<p><b><u>1 Demonetisation of Misinformation:</u></b></p> <p>Relevant Signatories participating in ad placements, commit to defund the dissemination of Disinformation, and improve the policies and systems which determine the eligibility of content to be monetised, the controls for monetisation and ad placement, and the data to report on the accuracy and effectiveness of controls and services around ad placements.</p>	<p><b><u>Measure 1.1.1 [adapted]:</u></b> Relevant Signatories involved in the selling of advertising, inclusive of media platforms, publishers and ad tech companies, will deploy, disclose, and enforce policies with the aims of:</p> <ul style="list-style-type: none"> <li>- first avoiding the publishing and carriage of harmful Disinformation to protect the integrity of advertising supported businesses</li> <li>- second taking meaningful enforcement and remediation steps to avoid the placement of advertising next to Disinformation content or on sources that repeatedly violate these policies</li> </ul>	<p><b><u>QRE 1.1.1:</u></b> Signatories will disclose and outline the policies they develop, deploy, and enforce to meet the goals of Measure 1.1 and will link to relevant public pages in their help centres.</p> <p><b><u>SLI 1.1.1 [adapted]:</u></b> Signatories will report, quantitatively, on actions they took to enforce each of the policies mentioned in the qualitative part of this service level indicator. This could include, for instance, actions to remove, to block, or to otherwise restrict advertising on pages and/or domains that disseminate harmful Disinformation.</p>
	<p><b><u>Measure 1.2.1:</u></b> Relevant Signatories responsible for the selling of advertising, inclusive of publishers,</p>	<p><b><u>QRE 1.2.1:</u></b> Signatories will outline their processes for reviewing, assessing,</p>

	<p>media platforms, and ad tech companies, will tighten eligibility requirements and content review processes for content monetisation and ad revenue share programmes on their services as necessary to effectively scrutinise parties and bar participation by actors who systematically post content or engage in behaviours which violate policies mentioned in Measure 1.1 that tackle Disinformation.</p>	<p>and augmenting their monetisation policies in order to scrutinise and bar participation by actors that systematically provide harmful Disinformation.</p>
	<p><b>Measure 1.5.1:</b> Relevant Signatories involved in the reporting of monetisation activities inclusive of media platforms, ad networks, and ad verification companies will take the necessary steps to give industry-recognised relevant independent third-party auditors commercially appropriate and fair access to their services and data in order to:</p> <ul style="list-style-type: none"> <li>- First, confirm the accuracy of first party reporting relative to monetisation and Disinformation, seeking alignment with regular audits performed under the DSA.</li> <li>- Second, accreditation services should assess the effectiveness of media platforms' policy enforcement, including Disinformation policies.</li> </ul>	<p><b>QRE 1.5.1:</b> Signatories that produce first party reporting will report on the access provided to independent third-party auditors as outlined in Measure 1.5 and will link to public reports and results from such auditors, such as MRC Content Level Brand Safety Accreditation, TAG Brand Safety certifications, or other similarly recognised industry accepted certifications.</p> <p><b>QRE 1.5.2:</b> Signatories that conduct independent accreditation via audits will disclose areas of their accreditation that have been updated to reflect needs in Measure 1.5.</p>
<p><b>3 Cooperation with Relevant Players:</b> Relevant Signatories involved in buying, selling and placing digital advertising commit to exchange best practices and strengthen cooperation with relevant players, expanding to</p>	<p><b>Measure 3.1:</b> Relevant Signatories will cooperate with platforms, advertising supply chain players, source-rating services, services that provide indicators of trustworthiness, fact-checking organisations, advertisers and any other actors active in the online monetisation value chain, to facilitate the integration and flow of information, in particular information</p>	<p><b>QRE 3.1.1:</b> Signatories will outline how they work with others across industry and civil society to facilitate the flow of information that may be relevant for tackling purveyors of harmful Disinformation.</p>

<p>organisations active in the online monetisation value chain, such as online e-payment services, e-commerce platforms and relevant crowd-funding/donation systems, with the aim to increase the effectiveness of scrutiny of ad placements on their own services.</p>	<p>relevant for tackling purveyors of harmful Disinformation, in full respect of all relevant data protection rules and confidentiality agreements.</p>	
	<p><u>Measure 3.2:</u> Relevant Signatories will exchange among themselves information on Disinformation trends and TTPs (Tactics, Techniques, and Procedures), via the Code Task-force, GARM, IAB Europe, or other relevant fora. This will include sharing insights on new techniques or threats observed by Relevant Signatories, discussing case studies, and other means of improving capabilities and steps to help remove Disinformation across the advertising supply chain - potentially including real-time technical capabilities.</p>	<p><b>QRE 3.2.1:</b> Signatories will report on their discussions within fora mentioned in Measure 3.2, being mindful of not disclosing information that is confidential and/or that may be used by malicious actors to circumvent the defences set by Signatories and others across the advertising supply chain. This could include, for instance, information about the fora Signatories engaged in; about the kinds of information they shared; and about the learnings they derived from these exchanges.</p>
	<p><u>Measure 3.3:</u> Relevant Signatories will integrate the work of or collaborate with relevant third-party organisations, such as independent source-rating services, services that provide indicators of trustworthiness, fact-checkers, researchers, or open-source investigators, in order to reduce monetisation of Disinformation and avoid the dissemination of advertising containing Disinformation.</p>	<p><b>QRE 3.3.1:</b> Signatories will report on the collaborations and integrations relevant to their work with organisations mentioned.</p>

**Provide reasoning for the choice of commitments and measures, as well as future plans (if applicable)**

*We prohibit Harmful Misinformation Actors from operating on Twitch, which includes all forms of monetization, including advertising. Additionally, we prohibit all political and issue advertising under our ads content policies. We work with internationally recognized advertising orgs such as GARM (Global Alliance for Responsible Media) to comply with common brand safety standards, including those related to misinformation and disinformation. However, we cannot commit to some of the specific measures involving verification of ads landing pages or fact checking of content, as this is not aligned with our Actor approach to misinformation.*

### III Political Advertising

**List of adopted commitments and measures**

**Qualitative reporting elements and service level indicators**

**Provide reasoning for the choice of commitments and measures, as well as future plans (if applicable)**

*Under our policies we prohibit ads content that is 'political, such as campaigns for or against a politician or a political party, or related to an election, or content related to issues of public debate.' Therefore the political advertising commitments related to political content labelling, identity verification, and user-facing transparency are not relevant to our service.*

### IV. Integrity of the Service

**List of adopted commitments and measures**

**Qualitative reporting elements and service level indicators**

**14 Manipulative Behaviours**

[adapted]:

In order to limit impermissible manipulative behaviours and practices

Measure 14.1:

Relevant Signatories will adopt, reinforce and implement clear policies regarding impermissible

**QRE 14.1.1:** Relevant Signatories will list relevant policies and clarify how they relate to the threats

<p>across their services, Relevant Signatories commit to put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of manipulative behaviours, actors and practises not permitted on their services.</p>	<p>manipulative behaviours and practices on their services, based on the latest evidence on the conducts and tactics, techniques and procedures (TTPs) employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework.</p>	<p>mentioned above as well as to other Disinformation threats.</p> <p><b>QRE 14.1.2:</b> Signatories will report on their proactive efforts to detect impermissible content, behaviours, TTPs and practices relevant to this commitment.</p>
<p>Such behaviours and practises, which should periodically be reviewed in light with the latest evidence on the conducts and TTPs employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework, may include:</p> <ul style="list-style-type: none"> <li>- The creation and use of fake accounts, account takeovers and bot-driven amplification,</li> <li>- Hack-and-leak operations,</li> <li>- Impersonation,</li> <li>- The purchase of fake engagements,</li> </ul>	<p><b>Measure 14.2 [adapted]:</b> Relevant Signatories will keep a detailed, up-to-date list of their publicly available policies that clarifies behaviours and practices that are prohibited on their services, and will outline in their reports how their respective policies and their implementation address the above set of TTPs, threats and harms as well as other relevant threats. The list of TTPs will serve as the base for the TTPs to be reported upon and relevant signatories will work within the Permanent Task-force to further develop and refine related indicators on the impact/effectiveness of their related actions.</p>	<p><b>QRE 14.2.1 [adapted]:</b> Relevant Signatories will report on actions taken to implement the policies they list in their reports and covering the range of TTPs identified/employed</p> <p><b>SLI 14.2.1 [adapted]:</b> Number of instances of identified TTPs and actions taken under policies addressing each of the TTPs as well as information on the type of content.</p>
<ul style="list-style-type: none"> <li>- Non-transparent paid messages or promotion by influencers,</li> <li>- The creation and use of accounts that participate in coordinated inauthentic behaviour, <ul style="list-style-type: none"> <li>- User conduct aimed at artificially</li> </ul> </li> </ul>	<p><b>Measure 14.3:</b> Relevant Signatories will convene via the Permanent Taskforce to agree upon and publish a list and terminology of TTPs employed by malicious actors, which should be updated on an annual basis, and</p>	<p><b>QRE 14.3.1 [adapted]:</b> Signatories will report on the list of TTPs agreed in the Permanent Task-force within 6 months of the signing of the Code and will update this list at least every year. They will also report about the common baseline</p>

<p>amplifying the reach or perceived public support for disinformation.</p>	<p>consist in a shared understanding of manipulative behaviours and practices not permitted on their service to-date. On that basis, they will aim to develop common baseline elements, objectives, and benchmarks for the policies and measures deployed to counter such manipulative behaviours and practices.</p>	<p>elements, objectives and benchmarks for the policies and measures.</p>
<p><b><u>16 Cooperation and Transparency:</u></b> Relevant Signatories commit to operate channels of exchange between their relevant teams in order to proactively share information about cross-platform influence operations, foreign interference in information space and relevant incidents that emerge on their respective services, with the aim of preventing dissemination and resurgence on other services, in full compliance with privacy legislation and with due consideration for security and human rights risks.</p>	<p><b><u>Measure 16.1</u></b> Relevant Signatories will share relevant information about cross-platform information manipulation, foreign interference in information space and incidents that emerge on their respective services for instance via a dedicated sub-group of the permanent Task-force or via existing fora for exchanging such information.</p>	<p><b><u>QRE 16.1.1:</u></b> Relevant Signatories will disclose the fora they use for information sharing as well as information about learnings derived from this sharing.</p> <p><b><u>SLI 16.1.1:</u></b> Number of actions taken as a result of the collaboration and information sharing between signatories. Where they have such information, they will specify which Member States that were affected (including information about the content being detected and acted upon due to this collaboration).</p>
	<p><b><u>Measure 16.2:</u></b> Relevant Signatories will pay specific attention to and share information on the tactical migration of known actors of misinformation, disinformation and information manipulation across different platforms as a way to circumvent moderation policies, engage different audiences or</p>	<p><b><u>QRE 16.2.1:</u></b> As a result of the collaboration and information sharing between them, Relevant Signatories will share qualitative examples and case studies of migration tactics employed and advertised by such actors on their platforms as observed by their moderation team and/or external partners from Academia or fact-checking organisations engaged in such monitoring.</p>



	coordinate action on platforms with less scrutiny and policy bandwidth.	
<p><b>Provide reasoning for the choice of commitments and measures, as well as future plans</b> (if applicable)</p> <p><i>Integrity of our service is the core of our approach to Trust and Safety on Twitch. We have a variety of policies and processes designed to combat bad actor behaviour, including Spam, Impersonation, Account Compromise, and Harmful Misinformation Actors. However, Twitch is a unique live platform where users stream themselves, their surroundings, or their own screens, all in real time. The creation of content is spontaneous and, unlike pre-produced and uploaded content, it cannot be edited before dissemination. We therefore do not have the technical capability to detect AI-generated manipulated content (Deepfakes), nor do we think it is currently feasible to build for our service. Additionally, as part of our current transparency reporting efforts, we detail the reports we receive, the violations we detect and remove, but we do not yet have reliable data granularity at the member state level, nor are more traditional metrics (likes, shares, comments) relevant to our service.</i></p>		

<b>V Empowering Users</b>		
<b><u>List of adopted commitments and measures</u></b>		<b><u>Qualitative reporting elements and service level indicators</u></b>
<p><b><u>17 Enhancing Media Literacy:</u></b></p> <p>In light of the European Commission’s initiatives in the area of media literacy, including the new Digital Education Action Plan, Relevant Signatories commit to continue and strengthen their efforts in the area of media literacy and critical thinking, also with the</p>	<p><b><u>Measure 17.1:</u></b></p> <p>Relevant Signatories [Twitch] will implement or continue to maintain tools to improve media literacy and critical thinking, for instance by empowering users or with guidance on how to evaluate online content. Twitch will partner with media literacy experts to develop these tools and promote the content on their service, including in relevant member-states.</p>	<p><b><u>QRE 17.1.1 [adapted]:</u></b> Relevant Signatories will outline the tools they develop or maintain that are relevant to this commitment and report on their deployment.</p> <p><b><u>SLI 17.1.1 [adapted]:</u></b> Relevant Signatories will report on metrics pertinent to assessing the effects of the tools described in the qualitative reporting element for Measure 17.1, which will include: the total count of impressions of the</p>

<p>aim to include vulnerable groups.</p>	<p>17.2 Relevant Signatories will develop, promote and/or support or continue to run activities to improve media literacy and critical thinking such as campaigns to raise awareness about Disinformation, as well as the TTPs that are being used by malicious actors, among the general public across the European Union, also considering the involvement of vulnerable communities.</p>	<p>tool; and information on the interactions/engagement with the tool.</p> <p><b>QRE 17.2.1 [adapted]:</b> Relevant Signatories will describe the activities they launch or support. Relevant signatories will further report on actions taken to promote the campaigns to their user base.</p>
<p><b><u>18 ‘Safe design’ of the architecture of the services, transparent policies, and accountability of recommender systems</u></b></p> <p>Relevant Signatories commit to minimise the risks of viral propagation of misinformation or disinformation by adopting safe design practices as they develop their systems, policies, and features.</p>	<p><b>Measure 18.2:</b> Relevant Signatories will develop and enforce publicly documented, proportionate policies to limit the spread of harmful false or misleading information (as depends on the service, such as prohibiting, downranking, or not recommending harmful false or misleading information, adapted to the severity of the impacts and with due regard to freedom of expression and information); and take action on webpages or actors that persistently violate these policies.</p>	<p><b>QRE 18.2.1:</b> Relevant Signatories will report on the policies or terms of service that are relevant to Measure 18.2 and on their approach towards persistent violations of these policies.</p> <p><b>SLI 18.2.1:</b> Relevant Signatories will report on actions taken in response to violations of policies relevant to Measure 18.2. The metrics shall include:</p> <ul style="list-style-type: none"> <li>- Total number of violations</li> <li>- Meaningful metrics to measure the impact of these actions (such as their impact on the visibility of or the engagement with content that was actioned upon )</li> </ul>

<p><b><u>19 ‘Safe design’ of the architecture of the services, transparent policies, and accountability of recommender systems:</u></b></p> <p>[adapted] Relevant Signatories using recommender systems commit to make them transparent to the recipients regarding how the algorithms are expected to behave and the outcomes prioritised and deprioritized on behalf of users, and provide options to users about recommender systems, and make available information on those options.</p>	<p><b><u>Measure 19.1 [adapted]:</u></b> Relevant Signatories will make available to their users, in a clear, accessible and easily comprehensible manner, information outlining the main behaviours recommenders use and optimise for.</p>	<p><b><u>QRE 19.1.1 [adapted]:</u></b> Relevant Signatories will provide details of the policies and measures put in place to implement the above-mentioned measures accessible to EU users, especially by publishing information outlining the main behaviours recommenders use and optimise for.</p>
	<p><b><u>Measure 19.2:</u></b> Relevant Signatories will provide options for the recipients of the service to select and to modify at any time their preferred options for relevant recommender systems, including giving users transparency about those options.</p>	<p><b><u>SLI 19.2.1:</u></b> Relevant Signatories will provide aggregated information on effective user settings, such as the number of times users have actively engaged with these settings within the reporting period or over a sample representative timeframe, and clearly denote shifts in configuration patterns.</p>
<p><b><u>23 Functionality to flag harmful false and/or misleading information:</u></b></p> <p>Relevant Signatories commit to provide users with the functionality to flag harmful false and/or misleading information that violates Signatories policies or terms of service.</p>	<p><b><u>Measure 23.1:</u></b> Relevant Signatories will develop or continue to make available on all their services and in all Member States languages in which their services are provided a user-friendly functionality for users to flag harmful false and/or misleading information that violates Signatories’ policies or terms of service. The functionality should lead to appropriate, proportionate and consistent follow-up actions, in full respect of the freedom of expression.</p>	<p><b><u>QRE 23.1.1:</u></b> Relevant Signatories will report on the availability of flagging systems for their policies related to harmful false and/or misleading information across EU Member States and specify the different steps that are required to trigger the systems.</p>
	<p><b><u>Measure 23.2:</u></b> Relevant Signatories will take the necessary measures to ensure that this functionality is duly protected from human or</p>	<p><b><u>QRE 23.2.1:</u></b> Relevant Signatories will report on the general measures they take to ensure the integrity of their reporting and appeals</p>

	<p>machine-based abuse (e.g., the tactic of ‘mass-flagging’ to silence other voices).</p>	<p>systems, while steering clear of disclosing information that would help would-be abusers find and exploit vulnerabilities in their defences.</p>
<p><b><u>24 Transparent appeal mechanism:</u></b></p> <p>Relevant Signatories commit to inform users whose content or accounts has been subject to enforcement actions (content/accounts labelled, demoted or otherwise enforced on) taken on the basis of violation of policies relevant to this section (as outlined in Measure 18.2), and provide them with the possibility to appeal against the enforcement action at issue and to handle complaints in a timely, diligent, transparent, and objective manner and to reverse the action without undue delay where the complaint is deemed to be founded.</p>	<p><b><u>Measure 24.1:</u></b> Relevant Signatories commit to provide users with information on why particular content or accounts have been labelled, demoted, or otherwise enforced on, on the basis of violation of policies relevant to this section, as well as the basis for such enforcement action, and the possibility for them to appeal through a transparent mechanism.</p>	<p><b><u>QRE 24.1.1 [adapted]:</u></b> Relevant Signatories will report on the availability of their notification and appeals systems and provide details on the steps of the appeals procedure.</p> <p><b><u>SLI 24.1.1:</u></b> Relevant Signatories provide information on the number and nature of enforcement actions for policies described in response to Measure 18.2, the numbers of such actions that were subsequently appealed, the results of these appeals, information, and to the extent possible metrics, and publish this information on the Transparency Centre.</p>
<p><b>Provide reasoning for the choice of commitments and measures, as well as future plans (if applicable)</b></p> <p><i>At Twitch, we take a layered approach to Safety. We as Twitch provide a baseline of acceptable behaviour through our community guidelines and service-level safety processes. This includes both ML detection and our review and enforcement processes for</i></p>		

violating content. We also provide tools for creators to personalise their safety standards above and beyond our community guidelines. Similarly, we provide tools for viewers, such as mature flags, chat filters, and blocking of other users so that they can customise the content they encounter and interactions they have across the service.

The primary commitments we cannot cover under the 'Empowerment of Users' chapter relate to modifications to our recommendations systems based on misinformation content. Because our policy is not focused on fact checking individual pieces of content and instead takes a holistic approach to removing Harmful Misinformation Actors, we cannot build downranking or labelling to reduce virality of content. Similarly, because we do not engage in content-level fact checking we cannot commit to providing trustworthiness indicators for content.

Additionally, while we can commit to sharing information about our review and our enforcement process through our existing transparency reports, we cannot fully commit to the time and resource investment requested, nor can we commit to all of the specific metrics required.

<b>VI Empowering the Research Community</b>		
<b>List of adopted commitments and measures</b>		<b>Qualitative reporting elements and service level indicators</b>
<p><b><u>27 Governance structure for access to data for research proposes requiring additional scrutiny [adapted]:</u></b> Relevant Signatories commit to provide vetted researchers with access to data necessary to undertake research on Disinformation</p>	<p><b><u>Measure 27.4.1:</u></b> Relevant Signatories commit to engage in pilot programs towards sharing data with vetted researchers for the purpose of investigating Disinformation, without waiting for the independent third-party body to be fully set up. Such pilot programmes will operate in accordance with all applicable laws regarding the sharing/use of data. Pilots could explore facilitating research on content that was removed from the services of Signatories and the data retention period for this content.</p>	<p><b><u>QRE 27.4.1:</u></b> Relevant Signatories will describe the pilot programs they are engaged in to share data with vetted researchers for the purpose of investigating Disinformation. This will include information about the nature of the programs, number of research teams engaged, and where possible, about research topics or findings.</p>
<p><b>Provide reasoning for the choice of commitments and measures, as well as future plans (if applicable)</b></p>		

*Currently, we often work with researchers and subject matter experts to guide policy and decision making at Twitch. This includes our work with the Global Disinformation Index, who support our Harmful Misinformation Actor Policy, our Safety Advisory Council, and other experts who are constantly helping us develop and maintain our policies and Community Guidelines. As we grow, it remains a priority to develop these relationships further and work with academics and other experts to understand disinformation intervention methods on our service. However, we cannot commit the resourcing at this time to supporting all of the research initiatives outlined in the 'Empowering the Research Community' chapter.*

### **VII Empowering the Fact Checking Community**

**List of adopted commitments and measures**

**Qualitative reporting elements and service level indicators**

**Provide reasoning for the choice of commitments and measures, as well as future plans (if applicable)**

*Twitch's approach to misinformation involves identifying persistent harmful misinformation actors, whose online content focuses on spreading egregious misinformation. We work with external experts in the space, such as the Global Disinformation Index to understand trends in misinformation claims and identify dedicated actors. However, due to this actor-level approach, we do not fact check individual pieces of content (nor is this recommended due to the live nature of our platform and the latency involved in fact-checking). Therefore the commitments and measures outlined in the Empowering the Fact Checking Community are not relevant to our work.*

### **VIII Transparency Centre**

**List of adopted commitments and measures**

**Qualitative reporting elements and service level indicators**

<p><b><u>34 Transparency centre website:</u></b>  To ensure transparency and accountability around the implementation of this Code, Relevant Signatories commit to set up and maintain a publicly available common Transparency Centre website.</p>	<p><u>Measure 34.1:</u> Signatories establish and maintain the common Transparency Centre website, which will be operational and available to the public within 6 months from the signature of this Code.</p>	
	<p><u>Measure 34.2:</u> Signatories provide appropriate funding, for setting up and operating the Transparency Centre website, including its maintenance, daily operation, management, and regular updating. Funding contribution should be commensurate with the nature of the Signatories' activity and shall be sufficient for the website's operations and maintenance and proportional to each Signatories' risk profile and economic capacity.</p>	
	<p><u>Measure 34.3:</u> Relevant Signatories will contribute to the Transparency Centre's information to the extent that the Code is applicable to their services.</p>	
	<p><u>Measure 34.4:</u> Signatories will agree on the functioning and financing of the Transparency Centre within the Task-force, to be recorded and reviewed within the Task-Force on an annual basis.</p>	
	<p><u>Measure 34.5:</u> The Task-force will regularly discuss the Transparency Centre and assess whether adjustments or actions are necessary. Signatories commit to implement the actions and adjustments decided within the Task-force within a reasonable timeline.</p>	

<p><b>35 Relevant Information:</b> Signatories commit to ensure that the Transparency Centre contains all the relevant information related to the implementation of the Code's Commitments and Measures and that this information is presented in an easy-to-understand manner, per service, and is easily searchable.</p>	<p><u>Measure 35.1:</u> Signatories will list in the Transparency Centre, per each Commitment and Measure that they subscribe to, the terms of service and policies that their service applies to implement these Commitments and Measures.</p>	
	<p><u>Measure 35.2 [adapted]:</u> Signatories provide information on the implementation and enforcement of their policies per service.</p>	
	<p><u>Measure 35.3:</u> Signatories ensure that the Transparency Centre contains a repository of their reports assessing the implementation of the Code's commitments.</p>	
	<p><u>Measure 35.4:</u> In crisis situations, Signatories use the Transparency Centre to publish information regarding the specific mitigation actions taken related to the crisis.</p>	
	<p><u>Measure 35.5</u> Signatories ensure that the Transparency Centre is built with state-of-the-art technology, is user-friendly, and that the relevant information is easily searchable (including per Commitment and Measure). Users of the Transparency Centre will be able to easily track changes in Signatories' policies and actions.</p>	



	<p><u>Measure 35.6 [adapted]</u>: The Transparency Centre will enable users to easily access and understand the Service Level Indicators and Qualitative Reporting Elements tied to each Commitment and Measure of the Code for each service, in a standardised and searchable way. The Transparency Centre should also enable users to easily access and understand Structural Indicators for each Signatory.</p>	
<p><b>36 Updating Relevant Information:</b> Signatories commit to updating the relevant information contained in the Transparency Centre in a timely and complete manner.</p>	<p><u>Measure 36.1:</u> Signatories provide updates about relevant changes in policies and implementation actions in a timely manner, and in any event no later than 30 days after changes are announced or implemented.</p>	
	<p><u>Measure 36.2:</u> Signatories will regularly update Service Level Indicators, reporting elements, and Structural Indicators, in parallel with the regular reporting foreseen by the monitoring framework. After the first reporting period, Relevant Signatories are encouraged to also update the Transparency Centre more regularly.</p>	
	<p><u>Measure 36.3:</u> Signatories will update the Transparency Centre to reflect the latest decisions of the Permanent Task-force, regarding the Code and the monitoring framework.</p>	<p><b>QRE 36.1.1 (for the Commitments 34-36):</b> With their initial implementation report, Signatories will outline the state of development of the Transparency Centre, its functionalities, the information it contains, and any other relevant information about its</p>

		<p>functioning or operations. This information can be drafted jointly by Signatories involved in operating or adding content to the Transparency Centre.</p> <p><b><u>QRE 36.1.2 (for the Commitments 34-36):</u></b> Signatories will outline changes to the Transparency Centre’s content, operations, or functioning in their reports over time. Such updates can be drafted jointly by Signatories involved in operating or adding content to the Transparency Centre.</p> <p><b><u>SLI 36.1.1 (for the Commitments 34-36):</u></b> Signatories will provide meaningful quantitative information on the usage of the Transparency Centre, such as the average monthly visits of the webpage.</p>
<p><b>Provide reasoning for the choice of commitments and measures, as well as future plans (if applicable)</b></p> <p><i>Twitch will contribute to the Transparency Centre in a way that is proportionate to our resources, size, and risk profile.</i></p>		

<b>IX Permanent Task Force</b>	
<b>List of adopted commitments and measures</b>	<b>Qualitative reporting elements and service level indicators</b>

<p><b>37 Participation in Permanent Task Force:</b> Signatories commit to participate in the permanent Task-force. The Task-force includes the Signatories of the Code and representatives from EDMO and ERGA. It is chaired by the European Commission, and includes representatives of the European External Action Service (EEAS). The Task-force can also invite relevant experts as observers to support its work. Decisions of the Task-force are made by consensus.</p>	<p><u>Measure 37.1:</u> Signatories will participate in the Task-force and contribute to its work. Signatories, in particular smaller or emerging services will contribute to the work of the Task-force proportionate to their resources, size and risk profile. Smaller or emerging services can also agree to pool their resources together and represent each other in the Task-force. The Task-force will meet in plenary sessions as necessary and at least every 6 months, and, where relevant, in subgroups dedicated to specific issues or workstreams.</p>	
	<p><u>Measure 37.2 [adapted]:</u> Signatories agree to work in the Task-force in particular – but not limited to – on the following tasks:</p> <ul style="list-style-type: none"> <li>- Establishing a risk assessment methodology and a rapid response system to be used in special situations like elections or crises.</li> <li>- Cooperate and coordinate their work in special situations like elections or crisis</li> <li>- Agree on the harmonised reporting templates for the implementation of the Code's Commitments and Measures, the refined methodology of the reporting, and the relevant data disclosure for monitoring purposes.</li> <li>- Review the quality and effectiveness of the harmonised reporting templates, as well as the formats and methods of data disclosure for</li> </ul>	

	<p>monitoring purposes, throughout future monitoring cycles and adapt them, as needed.</p> <ul style="list-style-type: none"><li>- Contribute to the assessment of the quality and effectiveness of Service Level and Structural Indicators and the data points provided to measure these indicators, as well as their relevant adaptation.</li><li>- Refine, test and adjust Structural Indicators and design mechanisms to measure them.</li><li>- Agree, publish and update a list of TTPs employed by malicious actors, and set down baseline elements, objectives and benchmarks for Measures to counter them, in line with the Chapter IV of this Code.</li><li>- Seek out and discuss research, expert input and up-to-date evidence relevant to the Code's commitments, such as, <i>inter alia</i>, emerging best practices in safe design, retroactive flagging, repository of fact-checks, provenance tools.</li><li>- Discuss and provide guidance on the adequate quantitative information to be provided by signatories to fulfil their reporting obligations regarding agreements with fact-checking organisations across different services.</li><li>- Regularly discuss whether the Code's Commitments and Measures need updating in view of technological, societal, market and legislative developments, as well as in view of accommodating new signatories and, where the Task-force agrees to be necessary, carry out such updates.</li></ul>	
--	--	--

	<ul style="list-style-type: none"> <li>- Review the appropriateness and consistency of adapted Measures for smaller or emerging services.</li> <li>- Promote the Code among relevant peers and integrate new Signatories to the Code.</li> </ul>	
	<p><u>Measure 37.3:</u> The Task-force will agree on and define its operating rules, including on the involvement of third-party experts, which will be laid down in a Vademecum drafted by the European Commission in collaboration with the Signatories and agreed on by consensus between the members of the Task-force.</p>	
	<p><u>Measure 37.4:</u> Signatories agree to set up subgroups dedicated to the specific issues related to the implementation and revision of the Code with the participation of the relevant Signatories.</p>	
	<p><u>Measure 37.5:</u> When needed, and in any event at least once per year the Task-force organises meetings with relevant stakeholder groups and experts to inform them about the operation of the Code and gather their views related to important developments in the field of Disinformation.</p>	
	<p><u>Measure 37.6:</u> Signatories agree to notify the rest of the Task-force when a Commitment or Measure would benefit from changes over time as their practices and approaches evolve, in view of technological, societal, market, and legislative developments. Having</p>	<p><b>QRE 37.6.1:</b> Signatories will describe how they engage in the work of the Task-force in the reporting period, including the sub-groups they engaged with.</p>

	discussed the changes required, the Relevant Signatories will update their subscription document accordingly and report on the changes in their next report.	
<p><b>Provide reasoning for the choice of commitments and measures, as well as future plans</b> (if applicable)</p> <p><i>Twitch will contribute to the task force in a way that is proportionate to our resources, size, and risk profile.</i></p>		

<b>X Monitoring the Code</b>		
<b>List of adopted commitments and measures</b>		<b>Qualitative reporting elements and service level indicators</b>
<p><b>38 Dedicate Adequate Resources:</b> The Signatories commit to dedicate adequate financial and human resources and put in place appropriate internal processes to ensure the implementation of their commitments under the Code.</p>		<p><b>QRE 38.1 [adapted]:</b> Relevant Signatories will outline the teams and internal processes they have in place, per service, to comply with the Code.</p>
<p><b>39 Providing Baseline Report:</b> Signatories commit to provide to the European Commission, within 1 month after the end of the implementation period (6 months after this Code's signature) the</p>		

<p>baseline reports as set out in the Preamble.</p>		
<p><b>40 Providing Regular Reports [adapted]:</b> Signatories commit to provide regular reporting on Service Level Indicators (SLIs) and Qualitative Reporting Elements (QREs). The reports and data provided should allow for a thorough assessment of the extent of the implementation of the Code's Commitments and Measures by each Signatory.</p>	<p><u>Measure 40.2 [adapted]:</u> Other Signatories will report yearly on the implementation of the Commitments and Measures taken under the present Code, including on the relevant QREs and SLIs.</p>	
	<p><u>Measure 40.3:</u> Signatories will regularly update the Transparency Centre with relevant QREs and SLIs, at least in line with their reporting period under this Code.</p>	
	<p><u>Measure 40.4:</u> Signatories will develop, within the Task-force, harmonised reporting templates.</p>	
	<p><u>Measure 40.5:</u> Signatories will regularly work to improve and optimise the monitoring and reporting framework of the Code, including the SLIs, within the Task-force, building in particular on feedback from the European Commission, ERGA and EDMO.</p>	
	<p><u>Measure 40.6 [adapted]:</u> Signatories will cooperate with the European Commission, respond to its reasonable requests and provide the European Commission with reasonable information, data and further input necessary to assess the implementation of the Code, allowing for the Code's efficient and thorough monitoring.</p>	
<p><b>42 Cooperate During Crisis:</b> Relevant Signatories commit to</p>		

<p>provide, in special situations like elections or crisis, upon request of the European Commission, proportionate and appropriate information and data, including ad-hoc specific reports and specific chapters within the regular monitoring, in accordance with the rapid response system established by the Task-force.</p>		
<p><b>43 Reporting Templates:</b> Signatories commit to produce reports and provide data following the harmonised reporting templates and refined methodology for reporting and data disclosure, as agreed in the Task-force.</p>		
<p><b>Provide reasoning for the choice of commitments and measures, as well as future plans (if applicable)</b></p> <p><i>Twitch will contribute to monitoring the code in a way that is proportionate to our resources, size, and risk profile.</i></p>		

*Signature*



Steve Bené  
General Counsel  
Twitch Interactive, Inc.

*Date and place*

13 June 2022  
San Francisco, California