A Guide to GIFCT Member Company Tools and Resources

GIFCT

Global Internet Forum to Counter Terrorism

Together for a Better Online World

Table of Contents

Introduction & How to Use This Document

This document serves as a guide for civil society groups, academic researchers, governments, and other tech companies wanting to know more about the resources and information that GIFCT member companies make available about their efforts to counter terrorist and violent extremist activity and tools developed to combat forms of online radicalization.

In each section we have linked directly to resources on each topic developed by GIFCT member companies as well as resources from GIFCT and its partners at the Global Network on Technology and Extremism (GNET) and Tech Against Terrorism.

To begin, this document maps each company's efforts that fulfill the GIFCT membership criteria. These are criteria that all tech companies must have publicly in place before being considered for GIFCT membership. First, companies must have **public content standards** that explicitly prohibit the promotion of terrorism and/or violent extremism in their terms of service, community guidelines, or other publicly available policies. This first section explores how companies discuss their frameworks for prohibiting the use of their platforms by terrorist and/or violent extremists.

The second section of this document links to member companies' **Transparency Reports**. All GIFCT member companies must publish transparency reports on at least an annual cadence. While we have seen larger GIFCT member companies continue to develop more granular and robust transparency reports, the initial development of such a report can be the most daunting piece of the GIFCT membership criteria for smaller companies.

The third section covers the **safety portals and wider safety information** that platforms make available so that their users are aware of the range of tools they can use to stay safe. Safety information is particularly crucial for activists, academics, journalists, and users that might be vulnerable to violent extremist groups. On some platforms, this information includes how to report hacked accounts, how to better ensure privacy in your account set-up, and how to flag abuse and harassment to the company.

The fourth section reviews the ways that GIFCT members ensure they have the ability to **receive and act on reports of illegal activity** or activity violating their terms of service from their users. This is also a GIFCT membership requirement. Reporting capabilities include internal flagging

tools, reporting portals, and outreach emails. These mechanisms vary across platforms based on how they operate. Whatever form it takes, it is important to ensure that the community using a platform can highlight abuses to that company that might be missed by any proactive detection efforts.

We know that content removal alone addresses a symptom and not the root causes of radicalization leading to violence. The fifth section of this document highlights resources related to GIFCT's membership criteria to support the capacity of civil society organizations to challenge violent extremism. Under this remit, some of the larger social media companies have developed international **counter-narrative programs and tooling** to help activists and NGOs scale and optimize their voices online as part of their efforts to push back on hate speech and extremism.

The final sections of this document highlights preventative measures to counter extremism online, specifically, **digital literacy training and tooling**. We have included, where available, open-access resources related to digital literacy along with relevant resources that guide activists and NGOs on how to utilize **advertising and marketing tools** to optimize the reach of their campaigns to their target audiences and how they can measure these efforts.

For ease of use, the appendix gives all the resource links in one comprehensive table by company, theme and URL link. GIFCT hopes that this document will serve as a useful resource and guide for better understanding and joint efforts in combating terrorism and violent extremism online.

Content Standards

Most platforms require users to agree to set terms of service before accessing a platform's tools. While terms of service give legal parameters for usage, content standards explain in a less legally formatted way what is and is not allowed to be shared on a given tech platform. These guidelines are put in place to ensure users can use the platforms freely and safely, while understanding where they might cross the line and have content removed or engagement on the platform restricted. These guidelines are generally global. Most companies design, review and update these standards based on feedback from a range of stakeholders that might include their users, government bodies, and global experts in fields such as technology, public safety and human rights. GIFCT members enforce their own respective policies and conduct their own practices in response to violations of their terms of service or standards such as content removal and account disabling.

A key piece of the GIFCT Membership criteria is that members must prohibit terrorist and/or violent extremist exploitation on their services and include this explicitly in their publicly-available terms of service or content standards. Just like governments, intergovernmental institutions, civil society organizations, and academics - tech companies often have slightly different definitions of "terrorism," "terrorist content" and "violent extremism." While there is no one globally agreed upon definition of terrorism or violent extremism, most tech companies, in their independent capacity, have developed definitions and approaches based on existing resources and in consideration of what will work best based on how their platforms operate.

Larger platforms often have content standards that address a range of harmful content and abuse related to violence and criminal behavior. For example, Facebook's dangerous individuals and organizations policy explicitly prohibits any organizations or individuals that proclaim a violent mission or are engaged violence to have a presence on their platform. This includes organizations or individuals involved in terrorist activity, organized hate, mass murder, organized violence and large-scale criminal activity. Likewise, Instagram's community guidelines outline a clear set of policies for what is and is not allowed on their platform. These guidelines explicity prohibit material that supports or praises terrorism, organized crime, or identified hate groups.

Also explicit in their guidelines, Twitter and YouTube do not allow violent organizations, including terrorist organizations, violent extremist groups, or individuals who affiliate with and promote the illicit activities of these groups to use their platforms for any purposes, including recruitment. These policies are part of the companies' respective sets of comprehensive guidelines against hate speech and harmful content.

Similarly, LinkedIn is committed to ensuring their platforms remain safe for all their users and do not tolerate content that depicts terrorist activity, that is intended to recruit for terrorist organizations, or threatens, promotes, or supports terrorism. To help guide users, LinkedIn provides publishing guidelines. In addition to prohibiting hate speech and content that advocates for violence against others, Microsoft's standards also prohibit terrorist content. This is defined as material posted by or in support of organizations included on the Consolidated United Nations Security Council Sanctions List that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups. JustPaste.It's Terms of Service prohibits terrorist content, which it defines as content in violation of EU Directives and EU Member State laws on terrorist offenses, or content produced by or

attributable to terrorist groups or entities designated by the European Union or by the United Nations.

Dropbox has put in place an Acceptable Use Policy page which explicitly condemns the use of their platform to publish or share materials that contain extreme acts of violence or terrorist activity, including terrorist propaganda. Similarly, MailChimp's Acceptable Use Policy is clear about suspending or terminating accounts which contain behavior, content, and in particular any campaigns promoting or supporting terrorism or violent extremism. Tumblr's Community Guidelines also state that the platform does not tolerate content that promotes, encourages, or incites acts of terrorism, including content which supports or celebrates terrorist organizations, their leaders, or associated violent activities.

WhatsApp's responsible use guide includes a video, a list of best practices, and what to avoid on the messaging platform. Though WhatsApp uses end-to-end encryption - meaning that the company does not have access to users' communications - it has clear reporting mechanisms and explicitly condemns illegal, obscene, defamatory, threatening, intimidating, harassing, hateful, racially, or ethnically offensive content. While MEGA's platform also features end-to-end encryption, its Terms of Service are explicit in not condoning, authorizing, supporting or facilitating the storage of any materials relating to violent extremism.

Platforms not typically considered to be social media platforms also recognize the importance of providing clear guidelines and rules to keep their users safe. For example, Amazon explicitly prohibits any activity that encourages or supports behavior that is illegal, including violence or content encouraging physical or financial harm, including terrorism. In Airbnb's trust and safety hub, its community standards refer to five pillars to guide its users: safety, security, fairness, authenticity and reliability. WordPress.com's User Guidelines clarify what is and is not allowed on user sites, while its Terrorist Activity page specifically explains how websites for United States government-designated terrorist groups and calls for violence are prohibited on websites that it hosts.

While the public tends to focus on the four to five larger GIFCT member companies, this criterion is necessary for all GIFCT members, large or small. Airbnb, Discord and Pinterest have reviewed and refreshed their Terms of Service and Community Guidelines through their membership process. While undergoing the GIFCT membership process, applying companies are given access to the Tech Against Terrorism Mentorship Program, sponsored by GIFCT. This supports tech companies who want to further develop policy language

references to terrorism and/or violent extremism in their Terms or Service or Community Guidelines to better combat terrorist use of their services.

In addition to the resources from Tech Against Terrorism, GIFCT also ensures there is a large body of academic and expert insights that members can review as they further develop their policies and understanding of how terrorist and violent extremists exploit online services. GIFCT works in close partnership with the Global Network on Extremism and Technology (GNET), an independent but GIFCT-funded global academic network. Topical insights, reports, and workshops with global experts are designed to highlight trends and adversarial shifts around the nexus between extremism and technology.

Transparency

In addition to explicit platform policies that prohibit terrorist and violent extremist content or activities, GIFCT members are required to publish an annual transparency report that reviews how it enforces its terms of use and standards. The format and categories in a transparency report vary from company to company, but most tend to provide data around government requests for information and wider efforts to enforce platform policies. As a company has more resources and the ability to build out nuanced metrics, reports sometimes include data on the appearance and removal of specific types of violating content. In the most advanced examples of transparency reporting to date these reports include rates of appeals and even the likelihood and rate at which users while on the platform may see violating content.

NGOs, academics, and governments can utilize this information to better understand how platforms enforce community standards, respond to violating content, and what the landscape of violating content looks like on a platform. This can inform how NGOs communicate about violent extremism on the platform.

Some of GIFCT's members include specific categories in their transparency data for terrorism and violent extremism, while others might have this information incorporated into other areas of violating or removed content. Member companies that include specific data on content flagged and/or removed for promoting terrorism are Facebook, JustPaste.It, Microsoft, Twitter, Wordpress.com and YouTube, based on their distinct, respective definitions of this content. These members are able to provide more granular data due to a number of different factors, including greater resources and additional personnel, as well as reporting by government entities, all of which support more robust efforts to detect, label, and review content.

Transparency reports also include data on the enforcement of content standards, requests for information or content removal by governments and law enforcement, as well as how content is restricted based on local laws. LinkedIn, MEGA, Mailchimp and Tumblr's transparency reports all feature a combination of these elements.

Transparency reports from GIFCT members Airbnb, Amazon, Pinterest and Dropbox primarily provide data focused on government and law enforcement requests due to how their platforms are set up and how on-platform abuse takes place. Discord's most recent transparency report focuses primarily on the company's responses to reports made by users, as well as efforts by the company to proactively enforce community standards by removing racist and extremist groups organizing on its servers without users first reporting the content to them.

Recognizing that tech companies, governments, and NGOs can always improve how they bring transparency to their work, GIFCT hosts a Transparency Working Group that brings together international, multi-sector stakeholders to foster better collaboration on how best to approach transparency in the context of tech platforms. This multi-sector effort ensures that GIFCT can best support its mission to facilitate dialogue between tech companies and other stakeholders on key issues.

For tech companies seeking membership that do not currently produce regular transparency reports, GIFCT provides guidance by connecting companies with our partner, Tech Against Terrorism, whose mentorship program facilitates developing best practices around transparency in a way that works for the specific platform. As a reminder, all platforms will naturally have different approaches to transparency reporting both in terms of frequency and data included. Some larger companies give transparency updates as often as quarterly, which would put a massive strain on capacities of smaller companies. As a reminder, depending on how a platform is set up, there might naturally be less data available to report on.

Finally, GIFCT has its own commitment to transparency and produces an annual Transparency Report, which documents our organization's growth, year's activities and progress in joint-tech innovations, and knowledge-sharing initiatives.

Safety Hubs

Often, activists, academics, journalists, and practitioners in the counterterrorism and counter-extremism space have to find ways to mitigate the risks to their personal safety online more than an average user. By using online platforms to research or challenge hate-based extremism and terrorism, an individual can often put themselves or the sensitive communities they engage with online at risk. Safety concerns also tend to arise for many activists and NGOs who often have public facing interactions with different communities and as a result tend to face several risks online. Platforms' safety guidelines and resources are, therefore, increasingly important to ensure that users know how to flag abuse, manage privacy settings, and report things such as potentially hacked accounts or nefarious activities of dangerous organizations.

Companies such as Discord, Facebook, Microsoft, and YouTube have extensive safety hubs that cover a wide range of abuse topics and risk mitigation best practices. For example, Discord provides account tips, server management and how to report problems directly to their Trust and Safety team as well as a Parents and Educators section. Facebook also ensures that its safety hubs cater to a range of different users, thereby addressing the needs of law enforcement, parents, and young people. Similarly, YouTube has safety resources focusing on online harms as well as parent, teen and educator resources.

Sometimes safety resources include third party facilitation and external experts to ensure safety measures develop as adversarial shifts occur. For example, Twitter has a dedicated Twitter account with the latest safety tools, resources, and updates to support its community. Twitter's Trust and Safety Council is a global group of independent expert organizations that look into a wide array of issues from online safety and harassment to human and digital rights. Twitter also provides tools geared towards brand safety. Meanwhile, platforms such as Facebook have a Safety Advisory Board, composed of leading internet safety organizations from around the world, who provide expertise, perspective, and insights that inform their approach to safety. The tools provided address a range of safety concerns, such as privacy measures and account security.

Instagram's Safety Hub provides comprehensive safety tools and a help center that gives safety guidelines. The center provides resources around privacy and security, reporting abuse, and digital wellbeing resources for its community. Microsoft's reports hub provides a Digital Safety Content Report that explicitly details their mechanisms for prohibiting certain content and conduct. In particular, it dedicates a significant section on what they do to help to prevent terrorists and violent extremists from exploiting digital platforms, including by addressing images and videos on their hosted services that include terrorist or violent extremist content.

WhatsApp aims to ensure that all users remain safe while using its platform through tools, including privacy controls and reporting mechanisms. It has also published a white paper on how WhatsApp prevents abuse of automated and bulk messaging. Similarly, MEGA provides users with a range of tools to remain safe across their different streams.

Dropbox and Pinterest, have developed principles and platform-specific approaches to tackle terrorist exploitation on their platforms with a focus on keeping users safe. Additionally, Airbnb provides safety guidance for both online and offline components of their service, providing users with proper information throughout their experience. On Airbnb's Trust and Safety page and in the Airbnb Host Resource Center, both hosts and travelers can learn more about the wider safety resources and information offered by the platform.

The evolution of safety tools and risk mitigation strategies also comes from external dialogues and international commitments with bodies such as the United Nations Counterterrorism Executive Directorate, the European Union Internet Forum, and the Christchurch Call to Action. GIFCT members Amazon, Facebook, Microsoft, Twitter and YouTube signed onto the Christchurch Call to Action in 2019 as part of their commitment to address the exploitation of technology by users looking to spread terrorist and violent extremist agendas online. These companies and GIFCT committed to a Nine-Point Plan for individual and collective action to prevent and respond to terrorist or violent extremist content.

In the GIFCT-funded Campaign Toolkit, there is also a Digital Security Checklist, which lays out the basics for digital security and steps to take if a campaign is threatened, harassed, or targeted by bad actors.

Overall, safety across digital platforms is a shared industry responsibility and efforts are furthered by a range of stakeholders including private sector, academic, civil society, governmental and intergovernmental actors. Multi-stakeholder engagement to further this is one of GIFCT's foundational goals. When different stakeholders work together to address this ever evolving and complex challenge, we see progress that would be difficult for any one entity to tackle alone.

Reporting Mechanisms

Related to broader safety concerns, another GIFCT membership requirement states that all members must have a functional way to "receive and act on

reports of illegal activity or activity violating terms of service." While members approach this in a variety of ways, all member companies provide public resources and tools to assist users in reporting illegal and prohibited activity and content.

At the very least a publicly available email address or direct contact portal is available, by which users may contact the company and report content or activity in violation of the platform's guidelines. Mailchimp, MEGA, and WhatsApp all provide outreach portals for this. For companies like MEGA and WhatsApp, which feature end-to-end encryption, this is the most efficient way to report abuse because the company does not otherwise have access to the content and activity of users. JustPaste.It users can directly email the platform at support@justpaste.it - instructions for properly submitting information about violating content can be found here.

In addition to outreach portals, other member companies use a combination of tools including content-adjacent reporting mechanisms and interactive online forms. Some larger companies have tools for giving more granular feedback on the type of abuse violating content might fall under. Many of these reporting tools also provide guidance on how to report content using the aforementioned content-adjacent mechanisms, ensuring that users are able to more easily report content in the future.

Discord, Dropbox, and Pinterest make use of general-purpose forms for reporting violating content. Discord requires users to share links to reported messages in their online form and provides instructions for users to do so successfully. In addition to their online forms, Dropbox and Pinterest also provide instructions for users to report content where it appears on the platform. Similarly, Wordpress.com's reporting mechanisms include on-platform options for users logged into Wordpress.com accounts and a form for users to directly contact the company. Amazon allows customers to report violating content via email and content adjacent reporting mechanisms. Information on both of these tools is located at the base of Amazon's Community Guidelines Page.

Airbnb provides guidance for reporting and blocking other users and reporting discrimination on their platform. Additionally, Airbnb provides users with a neighborhood support portal to call or chat with a representative about safety and broader neighborhood concerns.

Tumblr provides guidance to report blogs or offensive content where they are found on the platform, as well as a form for reporting by type of violation, including reporting suspected terrorist content.

Facebook, Instagram, LinkedIn, Microsoft and Twitter rely on similarly structured pages in their help centers to provide information about reporting mechanisms and instructions for how to report content, profiles, and other platform aspects. In addition to on-platform reporting resources, each of these companies also provides direct contact reporting options and guidance for reporting content without having an active user account.

Counter-Narrative Facilitation

While safety tools allow users to flag harm and on-platform violations that lead to possible removal of content, we also know that removal alone will never solve for the root causes of radicalization and hate-based extremism. Larger social media platforms have realized that their platforms also house crucial tools for activists and practitioners to develop content and online activities for prevention purposes. Some GIFCT members have developed tools that can optimize community-level voices that challenge hate speech and extremism. Supporting counterspeech and counter-narrative efforts emerges out of a recognition that deplatforming and removing content only addresses symptoms of radicalization, rather than causes.

Counterspeech efforts supported by tech companies often focus on helping activists and organizations produce, launch and evaluate localized content to challenge engaging narratives created by violent extremists. Other forms of counterspeech aim to create friction between individuals searching for violent extremist content by proactively surfacing alternative voices or local resources for disengagement. These efforts rely on strong partnerships between the tech companies and local civil society organizations around the world, reinforcing GIFCT's belief that multi-sector collaboration is a critical element of effectively combating extremism in online spaces.

Facebook's Counterspeech Hub houses a range of tips, tools, research and examples for activists and organizations to better understand Facebook's current initiatives and resources in the counterspeech space. The site's Initiatives page showcases the range of global projects, partnerships, and positive intervention approaches already underway. These include programs they run, such as the Redirect Initiative, as well as programs they have in partnership with bodies like the United Nations, such as Extreme Lives. The Counterspeech Resources section offers broader guidance for nonprofit organizations on how to take advantage of Facebook's tools and products, as well as more specific information on crafting counterspeech projects.

YouTube's Creators for Change program is a global initiative that partners with content creators from over 20 countries to promote positive messages, give

space to community voices, and empower youth voices as drivers of social good. Creators - known as Ambassadors and Fellows - receive mentorship and promotional assistance to work on Impact Projects, which engage viewers on a variety of challenging topics, including combating extremism, hate, and intolerance. YouTube was also an early pioneer of The Redirect Method, a tool created by Jigsaw and Moonshot CVE to "redirect" Google Search and YouTube users away from violent extremist recruitment content to YouTube videos that credibly refuted extremist content and recruitment materials. Modified versions of the initial pilot are being used across Microsoft, Facebook, and Instagram to address a variety of challenges.

To further foster this, GIFCT worked to gather resources that serve activists and organizations in their counterspeech efforts, working with ISD Global to produce the online Campaign Toolkit, a digital resource trove for anyone interested in producing and promoting counterspeech campaigns to global audiences. The Campaign Toolkit provides users with guidance as they develop campaigns and counter-narrative projects, as well as resources from many of our member companies to optimize the use of their platforms. Additionally, GIFCT hosts a Content-Sharing Algorithms, Processes, and Positive Interventions Working Group to ensure we further dialogues around best practices, monitoring and evaluation, and innovations.

To learn more about counterspeech and counter-narrative deployment, you can also look to our academic partners at the Global Network on Extremism and Technology (GNET) for published work by academics and researchers on this important and ever-evolving subject.

Digital Literacy

While counterspeech and counter-narrative campaigns and initiatives look to disrupt a cycle or pathway of hate-based radicalization, many practitioners and researchers have highlighted that preventing violent extremism needs to start with better comprehensive digital literacy for online audiences (young and old). Digital Literacy is a broad term that refers to a range of skills and information that allow individuals and organizations to safely and effectively operate in digital environments by questioning online information and having the tools to discern opinion from fact. While some of the material shared here is targeted at younger people, it is equally useful to those unfamiliar with operating on digital platforms and those who wish to engage younger audiences (activists, NGOs, teachers) by providing the basics in clear, straightforward language that can be easily communicated to others.

Some of our companies have built out substantial educational resources for digital literacy on their platforms and the internet at-large. Within Discord's Safety Center, users can find sections on "Controlling Your Experience" and a section for "Parents and Educators," which provide in-depth information for users to make their own experience safer. This also includes resources for those that might have responsibility for the safety of others on the platform.

Facebook hosts a Digital Literacy Library, which offers thorough modules for comprehension on several topics including; Security, Privacy and Reputation, and Community Engagement. Likewise, Instagram's Community page provides users with information about how the platform aims to protect its users, as well as a broad range of safety tools and programs to ensure safe, positive user experiences.

LinkedIn's Staying Safe page highlights best practices for LinkedIn users to maximize their use of the platform's products safely and effectively. The page also offers guidance for protecting personal information and resources for parents, educators and teenagers using the platform. Microsoft's digital literacy resources include two LinkedIn Learning courses, as well as a series of courses presented in a set of downloadable videos. Microsoft also hosts resources dedicated to Digital Civility online and open source Resources and Research.

Twitter, in collaboration with the United Nations Educational, Scientific and Cultural Organization (UNESCO), produced a document titled Teaching and Learning with Twitter: Media and Information Literacy. Additionally, A Safer Twitter, located within Twitter's Help Center, hosts a series of short videos that explain how to use some of the basic mechanisms offered on the platform to enhance the user's safety and experience.

Finally, YouTube provides a suite of Safety Resources, which cover a broad list of digital literacy subjects with specific information catering to parents, educators and teenagers. Additionally, YouTube also provides general-purpose resources for staying safe online and staying safe on YouTube, which educate users on phishing, account safety and basic mechanisms such as reporting and blocking.

Advertising and Marketing

Some GIFCT member companies offer advertising and marketing tools for their users based on how they function and monetize as a platform. While these tools are often developed for more traditional commerce and marketplace use cases, we also know that these tools can be optimized by activists, NGOs and practitioners to better launch their messaging to target audiences and further

counterspeech goals. Some companies have advertising and marketing tools to ensure that a range of organizations and/or activist's campaigns and voices reach the relevant target audiences and can be effectively measured.

For example, Facebook for Business is a free resource that allows small and medium businesses to expand their internet presence for greater visibility and reach. Meanwhile, the Facebook Social Impact site provides resources around a range of impact aimed streams: charitable causes, crisis response to vulnerable and affected people, health and mentorship.

The YouTube Advertising team helps organizations connect with their target audiences by supporting development content. YouTube Social Impact also helps users harness YouTube's scale, technology and talent to ignite and sustain movements that drive measurable social change. In this way YouTube also partners with others such as Google.org, Google for Nonprofits, Jigsaw and YouTube Creators For Change.

Twitter for business provides a range of free resources around campaign types, takeover products, advertising best practices and analytics. Especially for small businesses these are valuable tools on how to navigate their platform with recommendations, ideas and educational resources. Similarly, Microsoft provides a range of different open-source tools to support individuals, organizations, activist and business growth. Microsoft's Advertising provides insights, technology and proven expertise that empower organizations to deliver better-performing marketing campaigns. Microsoft Advertising Learning Lab offers free, on-demand, online learning courses to help users better understand the Microsoft Advertising interface. Finally, Microsoft Nonprofit ensures the benefits of world-class cloud technology is accessible and affordable for nonprofits. They provide nonprofit grants and discounts as well as industry-leading solutions help accelerate their impact. Microsoft provides step-by-step instructions to make this process as easy as possible.

Finally, above and beyond GIFCT member resources, additional resources include a Campaign Toolkit, which act as an information hub, providing activists and organizations with resources on a range of useful information, in particular for advertising, audience targeting and social good.

Appendix A: GIFCT Membership Criteria and Benefits

Membership Criteria

GIFCT member companies are listed on our website here. In order to join GIFCT, companies must meet the following requirements:

- Content standards that explicitly prohibit the promotion of terrorism in their terms of service, community guidelines, or other publicly available content policies
- The ability to receive and act on reports of illegal activity or activity violating terms of service
- A desire to explore new technical solutions to content and conduct challenges
- Regular, public data transparency
- A public commitment to respecting human rights, particularly free expression and privacy, when implementing content removal policies
- Support for expanding the capacity of civil society organizations to challenge violent extremism

If a company looking to join the GIFCT does not meet certain requirements, GIFCT offers that company mentorship through our partnership with Tech Against Terrorism.

Membership Benefits

- Potential access to GIFCT's hash-sharing database and URL sharing program
- Participation in crisis response communications around international terrorist and violent extremist events with online implications
- Briefings from scholars associated with the Global Network on Extremism and Technology (GNET), the academic research arm of GIFCT
- Briefings on technological approaches and solutions
- Priority participation in topical workshops, e-learnings and webinars with global experts

Contact: for any questions contact us at outreach@gifct.org.
Sign up to receive email updates from the Global Internet Forum to Counter Terrorism

Appendix B: Resources Index

GIFCT and Partner Resources

Partner	Webpage Title	Link
GIFCT	Membership Pillars	https://gifct.org/membership/
GIFCT	Transparency	https://gifct.org/transparency/
GIFCT	Working Groups	https://gifct.org/working-groups/
GIFCT	News Page and Newsletter Subscription	https://gifct.org/news/
GIFCT	Joint Tech Innovation	https://gifct.org/joint-tech-innovation/
GIFCT	Campaign Toolkit	https://www.campaigntoolkit.org/
GIFCT	Digital Security Checklist	http://campaigntoolkit.org/resources/campaign-toolkit-digital-security-check-list/
GIFCT	Email Updates	https://gifct.us17.list-manage.com/subscribe?u=6c63d1064a67c2bb2ac830e53&id=d458d7f692
TAT	Mentorship	https://www.techagainstterrorism.org/membership/tech-against-terrorism-mentorship/
TAT	Workshops and Events	https://www.techagainstterrorism.org/events/project-events/
TAT	Knowledge Sharing Platform (KSP)	https://ksp.techagainstterrorism.org/
GNET	Homepage: Insights and Reports	https://gnet-research.org/

GIFCT Member Resources

Member	Webpage Title	Link
Airbnb	Community Standards	https://www.airbnb.com/trust/standards
Airbnb	Transparency	https://news.airbnb.com/transparency/
Airbnb	Safety and accessibility	https://www.airbnb.com/help/topic/1398/safety-and-accessibility

Airbnb	Neighborhood Support	https://www.airbnb.com/neighbors
Airbnb	Trust and Safety	https://www.airbnb.com/trust
Airbnb	Host Resource Center	https://www.airbnb.com/resources/hosting-homes
Airbnb	How do I report a message or block someone on Airbnb?	https://www.airbnb.com/help/article/2020/how-do-i-report-a-message-or-block-someone-on-airbnb
Airbnb	How do I report discrimination to Airbnb?	https://www.airbnb.com/help/article/1433/how-do-i-report-discrimination-to-airbnb
Amazon	Community Guidelines	https://www.amazon.com/gp/help/customer/display.html?nodeId=GLHXEX85MENUE4XF
Amazon	Security and Privacy - Law Enforcement Information Requests	https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF
Amazon	Security and Privacy	https://www.amazon.com/gp/help/customer/display.html/ref=hp_bc_nav?ie=UTF8&nodeId=GRFTMVHP4HXMESSP
Discord	Community Guidelines	https://discord.com/guidelines
Discord	Transparency Report	https://blog.discord.com/discord-transparency-report-july-dec-2020-34087f9f45fb
Discord	Safety Center	https://discord.com/safety
Discord	Safety - Parents and Educators	https://discord.com/safety/360057166133-Working-with-CARU-to-protect-users-on-Discord
Discord	Trust and Safety - How to Properly Report Issues to Trust and Safety	https://support.discord.com/hc/en-us/articles/360000291932-How-to-Properly-Report-Issues-to-Trust-Safety
Dropbox	Acceptable Use Policy	https://www.dropbox.com/acceptable_use
Dropbox	Transparency Overview	https://www.dropbox.com/transparency
Dropbox	Security and Privacy - Report Abuse on Dropbox	https://help.dropbox.com/accounts-billing/security/report-abuse
Dropbox	Blog, 2019: Protecting our users and society: guarding against terrorist content	https://blog.dropbox.com/topics/company/protecting-our-users-and-society-

		-guarding-against-terrorist-con
Facebook	Community Standards	https://www.facebook.com/communitystandards/
Facebook	Transparency Report	https://transparency.facebook.com/
Facebook	Digital Literacy Library	https://www.facebook.com/safety/educators
Facebook	Community Standards - Dangerous Individuals and Organizations	https://www.facebook.com/communitystandards/dangerous_individuals_organizations
Facebook	Combating Hate and Extremism (FB News, 2019)	https://about.fb.com/news/2019/09/combating-hate-and-extremism/
Facebook	What Are We Doing to Stay Ahead of Terrorists? (FB News, 2018)	https://about.fb.com/news/2018/11/staying-ahead-of-terrorists/
Facebook	Business	https://www.facebook.com/business
Facebook	Facebook Counterspeech	https://counterspeech.fb.com/en/
Facebook	Social Impact	https://socialimpact.facebook.com/
Facebook	Safety Center	https://www.facebook.com/safety
Facebook	Safety Center - Law Enforcement	https://www.facebook.com/safety/groups/law
Facebook	Safety Center - Parents Portal	https://www.facebook.com/safety/parents
Facebook	Safety Center - Empowering Youth	https://www.facebook.com/safety/youth
Facebook	Safety Advisory Board	https://www.facebook.com/help/222332597793306/?ref=sc
Facebook	Policies and Reporting - How to Report Things	https://www.facebook.com/help/1380418588640631/how-to-report-things/?helpref=hc_fnav
Instagram	Community Guidelines	https://www.facebook.com/help/instagram/477434105621119
Instagram	Community Guidelines FAQs (Instagram Blog, 2018)	https://about.instagram.com/blog/announcements/instagram-community-guidelines-faqs
Instagram	Transparency Report	https://transparency.facebook.com/
Instagram	Help Center - Report Something	https://help.instagram.com/165828726894770/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Privacy%20and%20Safety%20Center&bc[2]=Report

		%20Something
Instagram	Community	https://about.instagram.com/community/
JustPaste.It	Terms of Service	https://justpaste.it/terms
JustPaste.It	Transparency Report	https://justpaste.it/transparency_report_2020
JustPaste.It	Abuse Reporting	https://justpaste.it/terms/reporting
LinkedIn	Professional Community Policies	https://www.linkedin.com/legal/professional-community-policies
LinkedIn	Transparency	https://about.linkedin.com/transparency
LinkedIn	Report Inappropriate Content, Messages, or Safety Concerns	https://www.linkedin.com/help/linkedin/answer/146/report-inappropriate-content-messages-or-safety-concerns?lang=en
LinkedIn	Safety Center - Identifying Abuse	https://safety.linkedin.com/identifying-abuse
LinkedIn	Safety Center - Staying Safe	https://safety.linkedin.com/staying-safe
Mailchimp	Acceptable Use Policy	https://mailchimp.com/legal/acceptable_use/
Mailchimp	Transparency Reports	https://mailchimp.com/transparency-report/
Mailchimp	Abuse Desk	https://mailchimp.com/contact/abuse/
MEGA	Terms of Service	https://mega.nz/terms
MEGA	Transparency Report 2020	https://mega.nz/Mega_Transparency_Report_202009.pdf
MEGA	Contact Us - Report Objectionable Material	https://mega.io/contact
MEGA	Takedown Guidance Policy	https://mega.io/takedown
Microsoft	Community Code of Conduct	https://answers.microsoft.com/en-us/page/codeofconduct
Microsoft	Report Hate Speech Content Posted to a Microsoft Hosted Consumer Service	https://www.microsoft.com/en-us/concern/hatespeech
Microsoft	Corporate Social Responsibility - Reports Hub	https://www.microsoft.com/en-us/corporate-responsibility/reports-hub
Microsoft	Digital Safety Content Report	https://www.microsoft.com/en-us/corporate-responsibility/digital-safety-content-report?activetab=pivot_1:primaryr

		4
Microsoft	Digital Literacy	https://www.microsoft.com/en-us/digitalliteracy
Microsoft	Report Terrorist Content Posted to a Microsoft Consumer Service	https://www.microsoft.com/en-us/concern/terroristcontent
Microsoft	Register with Microsoft Nonprofits	https://nonprofit.microsoft.com/en-us/getting-started
Microsoft	Advertising	https://about.ads.microsoft.com/en-gb/h/a/microsoft-advertising
Microsoft	About Microsoft Advertising	https://about.ads.microsoft.com/en-gb/get-started/about-microsoft-advertising
Microsoft	AI For Good	https://www.microsoft.com/en-us/ai/ai-for-good
Microsoft	Partner Network - Sales and Marketing	https://partner.microsoft.com/en-cy/marketing
Microsoft	Online Safety	https://www.microsoft.com/en-us/digital-skills/online-safety?activetab=protect-whats-important%3aprimaryr3
Microsoft	Online Safety - Resources and Research	https://www.microsoft.com/en-us/digital-skills/online-safety-resources
Microsoft	Security	https://www.microsoft.com/en-us/security
Microsoft	Report a Concern to Bing	https://www.microsoft.com/en-us/concern/bing
Microsoft	Advertising Learning Lab	https://learninglab.about.ads.microsoft.com/
Microsoft	Microsoft partners with Institute for Strategic Dialogue and NGOs to discourage online radicalization to violence (blog post, Microsoft on the Issues)	https://blogs.microsoft.com/on-the-issues/2017/04/18/microsoft-partners-institute-strategic-dialogue-ngos-discourage-online-radicalization-violence/
Microsoft	Corporate Citizenship - Support for NGOs	https://www.microsoft.com/en-hk/sparkhk/support-for-ngos
Microsoft	Advertising Training Courses	https://about.ads.microsoft.com/en-gb/resources/training/courses
Microsoft	Advertising - Ad products: Solutions for online advertising	https://about.ads.microsoft.com/en-gb/solutions/ad-products
Microsoft	Online Safety - Promoting Digital Civility	https://www.microsoft.com/en-us/digital-skills/digital-civility?activetab=dci_r

		eports:primaryr4
Microsoft	Request to Reinstate Disabled Content	https://www.microsoft.com/en-us/concern/reinstatecontent
Pinterest	Community Guidelines	https://policy.pinterest.com/en/community-guidelines
Pinterest	Transparency Report	https://help.pinterest.com/en/article/transparency-report
Pinterest	Help Center - Safety - Report Something on Pinterest	https://help.pinterest.com/en/article/report-something-on-pinterest
Pinterest	Help Center - Safety - Get More Help - Report a Policy Violation	https://help.pinterest.com/en/contact
Tumblr	Community Guidelines	https://www.tumblr.com/policy/en/community
Tumblr	Transparency Report	https://www.tumblr.com/transparency
Tumblr	Reporting Offensive Content	https://tumblr.zendesk.com/hc/en-us/articles/226270628-Reporting-offensive-content
Tumblr	Report Abuse	https://www.tumblr.com/abuse
Tumblr	Report Suspected Terrorism Content	https://www.tumblr.com/abuse/terrorism
Twitter	The Twitter Rules	https://help.twitter.com/en/rules-and-policies/twitter-rules
Twitter	NGO Handbook	https://about.twitter.com/content/dam/about-twitter/en/tfg/download/campaigning-on-twitter-handbook-2019.pdf
Twitter	Transparency	https://transparency.twitter.com/
Twitter	Safety and Security	https://help.twitter.com/en/safety-and-security
Twitter	Trust and Safety Council	https://about.twitter.com/en/our-priorities/healthy-conversations/trust-and-safety-council
Twitter	Brand Safety	https://business.twitter.com/en/help/ads-policies/brand-safety.html
Twitter	A Safer Twitter	https://help.twitter.com/en/a-safer-twitter
Twitter	Violent Organizations Policy	https://help.twitter.com/en/rules-and-policies/violent-groups
Twitter	How Twitter Ads Work	https://business.twitter.com/en/help/tr

		oubleshooting/how-twitter-ads-work.html
Twitter	Advertising - Targeting	https://business.twitter.com/en/advertising/targeting.html
Twitter	Advertising - Campaign Types	https://business.twitter.com/en/advertising/campaign-types.html
Twitter	Analytics	https://analytics.twitter.com/about
Twitter	Business Resources and Guides	https://business.twitter.com/en/resources.html
Twitter	Corporate Philanthropy	https://about.twitter.com/en/who-we-are/twitter-for-good
Twitter	Hateful Conduct Policy	https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy
Twitter	Q&A: The marketing team behind @SimonBooks shares tips on creating impactful organic and paid content (Blog Post, Twitter Business)	https://business.twitter.com/en/blog/marketing-team-behind-simonbooks.html
Twitter	@TwitterSafety (Twitter Account)	https://twitter.com/twittersafety
Twitter	Help - Safety and Security - Sensitive Content	https://help.twitter.com/en/safety-and-security#sensitive-content
Twitter	Business - Twitter Video Resources	https://business.twitter.com/en/resources/video.html
Twitter	Rules and Policies - Report Violations	https://help.twitter.com/en/rules-and-policies/twitter-report-violation
Twitter	Teaching and Learning with Twitter Media and Information Literacy	https://about.twitter.com/content/dam/about-twitter/en/tfg/download/teaching-learning-with-twitter-unesco.pdf
WhatsApp	How to Use WhatsApp Responsibly	https://faq.whatsapp.com/general/security-and-privacy/how-to-use-whatsapp-responsibly/?lang=en
WhatsApp	Safety Tips	https://www.whatsapp.com/safety
WhatsApp	Security	https://www.whatsapp.com/security
WhatsApp	White Paper - How WhatsApp Fights Bulk Messaging and Automated Behavior	https://scontent.whatsapp.net/v/t61.22868-34/69510151_652112781951150_6923638360331596993_n.pdf/Stopping-Abuse-white-paper.pdf?ccb=1-3&_nc_sid=2fbf2a&_nc_ohc=13FdwpNrR5kAX_lVl7K&_nc_ht=scontent.whatsapp.net&oh=4c0373c73d7d6360fde01d79e97

		2c38f&oe=6077C68F
WhatsApp	Help Center - Advanced Safety and Security Features - Report Issues to WhatsApp	https://faq.whatsapp.com/general/security-and-privacy/staying-safe-on-whatsapp/?lang=en
WordPress.com	Community Guidelines	https://wordpress.com/support/user-guidelines/
WordPress.com	Transparency Report	https://transparency.automattic.com/landing/
WordPress.com	Report a Site	https://wordpress.com/support/report-blogs/
WordPress.com	Report Content to WordPress.com Staff	https://wordpress.com/abuse/
WordPress.com	Terrorist Activity Policy	https://wordpress.com/support/terrorist-activity/
YouTube	Community Guidelines	https://www.youtube.com/howyoutubeworks/policies/community-guidelines/#community-guidelines
YouTube	Transparency - Community Guidelines Enforcement	https://transparencyreport.google.com/youtube-policy/removals?hl=en
YouTube	Safety Resources	https://support.google.com/youtube/topic/9386941?hl=en&ref_topic=2803240
YouTube	Safety Resources - Suicide and Self-Injury Policy	https://support.google.com/youtube/answer/2802245?hl=en&ref_topic=9386941
YouTube	Safety Resources - Parent Resources	https://support.google.com/youtube/answer/2802272?hl=en&ref_topic=9386941
YouTube	Safety Resources - Teen Resources	https://support.google.com/youtube/answer/2802244?hl=en&ref_topic=9386941
YouTube	Safety Resources - Educator Resources	https://support.google.com/youtube/answer/2802327?hl=en&ref_topic=9386941
YouTube	Policies - Violent Criminal Organizations	https://support.google.com/youtube/answer/9229472?hl=en&ref_topic=9282436
YouTube	Help - Hate Speech Policy	https://support.google.com/youtube/answer/2801939?hl=en-GB
YouTube	Advertising	https://www.youtube.com/intl/en-GB/

		ads/
YouTube	Creators for Change	https://www.youtube.com/creators-for-change/
YouTube	YouTube Nonprofit Program	https://www.google.com/nonprofits/offerings/youtube-nonprofit-program/
YouTube	Social Impact	https://socialimpact.youtube.com/
YouTube	Help Center - Report Inappropriate Content	https://support.google.com/youtube/answer/2802027?hl=en&ref_topic=9387085
YouTube	Help Center - Other Reporting Options	https://support.google.com/youtube/answer/2802057?hl=en&ref_topic=9387085
YouTube	Help Center - Report a YouTube search prediction	https://support.google.com/youtube/answer/7626105?hl=en&ref_topic=9387085
YouTube	Help Center - Trusted Flagger Program	https://support.google.com/youtube/answer/7554338?hl=en&ref_topic=9387085
YouTube	Ever wonder how YouTube works?	https://www.youtube.com/intl/ALL_uk/howyoutubeworks/