Home Office

Interim Code of Practice on Terrorist Content and Activity Online

December 2020

Contents

Overview of the interim code

S1 PRINCIPLE 1

Companies seek to identify and prevent terrorist content and activity from being accessible to UK users on their services.

S1 PRINCIPLE 2

Companies seek to minimise the potential for searches to return results linking to terrorist content and activity.

S2 PRINCIPLE 3

Companies facilitate and participate in industry collaboration to promote holistic and effective approaches to tackling terrorist use of the internet.

S3 PRINCIPLE 4

Companies seek to implement effective user reporting, complaints and timely redress processes to ensure users are empowered and protected.

S4 PRINCIPLE 5

Companies seek to support investigation and prosecution of individuals for terrorist offences in the UK in line with existing legal frameworks and voluntary reporting measures.

Introduction
Interim Code of Practice on Terrorist Content and Activity Online

The global reach of the internet continues to be exploited by terrorists to distribute content and engage in activity designed to aid and abet terrorist attacks, radicalise and recruit vulnerable people and provide a place for supporters to meet virtually. Terrorist use of the internet can pose severe real-world harms to people, property and UK interests:

- There has been an enormous growth in the volume of terrorist content and activity online.
- The availability and dissemination of terrorist content and activity online has been shown to have inspired terrorist attacks taking place on UK soil and against UK nationals and interests overseas. Almost all UK terrorist attack planners from 2012-2017 downloaded, shared or consumed content and activity associated with terrorism and extremism online.
- Online content is seen across terrorism investigations, including cases where suspects have become very quickly radicalised to the point of planning attacks.

While some companies have made notable progress to tackle terrorist content and activity online – both domestically and internationally – it is important to recognise that the threat posed by it is constantly evolving, as are the technology and methods used to tackle it. The response by industry to this threat must be agile - continually reviewed and improved as the threat landscape changes.

Recognising that terrorist use of the internet is a global challenge, the government has sought to align with and enhance the global approach to Preventing Terrorist Use of the Internet (PTUI) through this interim code. This has meant considering and building upon current international initiatives and agreements, such as the Christchurch Call to Action and the commitments of the Global Internet Forum to Counter Terrorism (GIFCT), alongside carrying out extensive consultation with international partners to exchange learning and support coordinated and complementary approaches.

This interim code provides detailed guidance for companies to help them understand how to mitigate the range of risks arising from online terrorist content and activity in order to protect their users and the general public from harm. The code is underpinned by five principles for companies to work towards, with examples of how a company might achieve this and includes supporting information in appendices 1-3. The guidance is for companies that supply services or tools which allow, enable or facilitate users to share or discover **user-generated content**[1] or to interact with each other online.

We encourage all companies to be proactive and ambitious in how they consider and implement the recommendations within this interim code of practice.

1 *See definition in Appendix 1*

Purpose of the interim codes of practice

The Online Harms White Paper committed the government to produce two voluntary interim codes of practice setting out the action companies are encouraged to take to address terrorism and child sexual exploitation and abuse online ahead of the regulator becoming operational and issuing full codes of practice.

The Interim Code of Practice on Online Child Sexual Exploitation and Abuse will be released in tandem with this code. While the two codes are designed to align with one another as much as possible to assist companies with understanding and implementing both codes, there are some differences as they respond to two different threats.

The interim codes and all the principles contained within them are voluntary and non-binding. Companies should consider factors such as the nature of their services, the underlying architecture of their systems, the risks to their users, and the availability of established or emerging technologies appropriate for addressing the issues identified.

The principles are not reliant on the online harms legislation and all of the measures outlined in this interim code are steps that companies can take now, either on a voluntary basis or under existing legal frameworks. The measures are designed to take account of existing exemptions in these frameworks for journalistic or academic research purposes, and to complement broader international commitments to address terrorism online. Government will work with the online harms regulator so that appropriate learning from companies' experience in adopting measures that are recommended in this interim code can inform the development of the regulator's codes of practice.

The aims and examples of good practice under each principle are intended to set out for all companies (including small to medium sized enterprises - see Appendix 3) action that can be taken to address the terrorist threat on a wide range of services and to allow companies to begin to prepare for the codes of practice, which will be produced by the regulator once it is in place.

This interim code of practice is designed to be read in parallel with the Full Government Response to the Online Harms White Paper. It reflects the expectations set out in the White Paper and seeks to mitigate a range of risks posed by terrorist content and activity online, building on existing industry and government-led initiatives.

As far as possible, this interim code of practice takes into account how the future online harms regulation is likely to work, as set out in the Full Government Response. By taking action to protect their users from this serious harm now, companies will be better prepared when the online harms legislation comes into force.

The UK is committed to protecting fundamental rights, including freedom of expression and privacy, as well as to a free, open and secure internet. To ensure protections for freedom of expression, the interim code provides guidance on best practice to address only illegal content and activity, rather than other content and activity that is not illegal but may cause harm.

Under the interim codes companies are encouraged to:

- have mechanisms for understanding the level and nature of threats on their services (as far as reasonably practicable), the impact of changes to systems, processes and policies they introduce, and remaining areas of high risk.
- take all reasonable steps to implement each principle in this interim code, where it is relevant for their services.
- review their existing safety processes and terms and conditions against each of the principles. Based on this review, identify and act on gaps in existing measures, or where existing measures can go further, for example by improving and investing in tools and/or moderation processes and innovating to address areas of risk.
- share information, best practice, and tools across industry, particularly with smaller companies, for example, through working collaboratively with industry bodies. Smaller companies are encouraged to proactively seek information, best practice and tools.
- be transparent about how the above steps have been actioned and, where appropriate, provide public reports, which may include content/account removal, user complaints received and user redress requests.

Section 1:
Identify, prevent and act on terrorist content and activity

PRINCIPLE 1: Companies seek to identify and prevent terrorist content and activity from being accessible[2] to UK users on their services.

Context: Terrorists place a huge premium on quickly communicating with their audiences and engage in cross-service efforts to generate maximum reach. It is therefore vital to ensure that (where proportionate and necessary to the threat) companies have robust mechanisms and processes in place to identify and remove terrorist content and activity, as well as preventing, where possible, re-uploads and new content being made available to users. Some companies already identify and remove terrorist content and activity from their services in response to reports from users, through referrals from law enforcement, or through detection by automated technologies and/or human-led measures, either at the point of or after upload.

2 *Prevent it being accessible in this context means to remove through hashing or other means, where possible, before other users can see/share/download it.*

Aims of the principle:

Under this principle companies should take reasonable steps to:

- seek to identify and prevent the upload of terrorist content and activity using proactive measures[3] such as automated technologies alongside human moderation.
- seek to remove content expeditiously and minimise the likelihood of this same content being made available again to other users from that point onwards, where companies are unable to identify terrorist content and activity until after upload (for example, due to the functionality or size of their services). This might involve proactive measures, as well as reviewing user reports and responding to referrals from law enforcement.

Companies should have appropriate safeguards to ensure that legitimate content (content which is legal and does not breach the company's terms and conditions) is not inadvertently prevented from being uploaded or removed (and having appropriate appeals mechanisms in place where this does happen).

Guidance is provided in Appendix 1 for companies to understand what terrorist content and activity on their services could look like.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- identify terrorist content and activity by developing in-house or integrating third-party automated tools including hash, URL and/or keyword lists, or through employing human moderators.
- review identified terrorist content and activity using an appropriate combination of technological and human-led measures.
- remove identified terrorist content and activity which is suspected[4] to be in breach of UK terrorism legislation.
- expeditiously identify and remove livestreamed terrorist activity, including through the use of technological and/or human moderation. This content should be removed whilst it is being livestreamed or as soon as possible thereafter.
- take appropriate action (e.g. to remove and to refer to law enforcement) on user accounts or profiles that disseminate or promote terrorism and terrorist content and activity.
- ensure company terms and conditions, safety policies and content moderation processes are informed by an up-to-date understanding of the online terrorist threat on their services.
- ensure regular and appropriate training for staff on the changing threat posed by terrorist use of the internet and how to identify such content and activity.
- offer support services to content moderators by making provision for the psychological assessment and welfare of staff viewing this distressing material.

3 Proactive measures are those which companies can take to identify, review and remove terrorist content and activity online, or otherwise minimise its accessibility to users, prior to being informed by others (including law enforcement, civil society organisations or users) of that content. These measures involve the use of automated technology and human moderation and are already an essential element of an effective response to tackling terrorist content online for some services.

4 See guidance in Appendix 1

PRINCIPLE 2: Companies seek to minimise the potential for searches to return results linking to terrorist content and activity.

Context: While search engines do not host content, they provide an online search service in relation to publicly available information locations comprising, at least in principle, all websites or all websites in a particular language. Search functionality within a service allows users to search for available content hosted by that service. Search engines and other services with in-built search functionality can allow or even encourage users to discover and access terrorist content and activity.

This principle is designed to apply to both companies whose services host content and encompass search functionality, as well as search engines who do not host content themselves.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- minimise the potential for search results linking to terrorist content and activity, including not allowing predictions (autocompletion) associated with terrorist content and activity.

The way companies apply this principle will depend on whether the service has in-built search functionality or is a search engine.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- ensure search activity for terrorist content does not promote access to relevant results by checking that:
  - autocomplete entries do not suggest for terrorist search terms. This will require that companies maintain an awareness of current terrorist search terms;
  - further terrorist content or accounts/ profiles are not suggested to users based on previous searches/interests; and
  - URLs to terrorist content are demoted or delisted.
- signpost users, where possible, to alternative sources of information or support when terrorist content search terms are used.
- develop or use in-house or third-party tools to identify terrorist content and search terms.
- keep lists of terms up to date as they are altered, or new terminology adopted.
- work collaboratively with industry to maintain lists of search terms.

Government recognises that in some circumstances, there might be good faith reasons for individuals searching for this type of content, and it is intended that this would fall within the existing exemptions for journalistic and academic research purposes within existing legal frameworks.

Section 2: Collaboration

PRINCIPLE 3: Companies facilitate and participate in industry collaboration to promote holistic and effective approaches to tackling terrorist use of the internet.

Context: Some companies already work with others to share helpful practices, tools and techniques via a range of collaborative forums. Companies should, where proportionate, participate in or expand this collaborative work, sharing insights, knowledge and information. This will result in a better understanding of the threat and provide support for ongoing initiatives to tackle terrorist content and activity online.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- commit to collaborative working with industry and with governments, academia and civil society in order to:
  - respond quickly to online aspects of emerging or active terrorist incidents, through the enacting of relevant crisis protocols or other internal processes for responding to incidents; and
  - engage with relevant industry bodies, which enable the sharing of knowledge and expertise to improve companies' capability to respond to terrorist content and activity online.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- participate in information exchange between companies in relation to terrorist content and activity and the evolving threat.[5]
- establish internal crisis response processes to respond to active terrorist incidents, to ensure relevant information is quickly and efficiently shared and acted on. This might include considering whether it is proportionate to participate in existing crisis protocols set up by cross-industry bodies, for example the GIFCT Content Incident Protocol.
- work collaboratively with partners across industry, government, academia and civil society to:
  - support the development of automated tools that aid efforts to tackle terrorist use of the internet;
  - use existing cross-industry capabilities such as hash lists to enable greater detection and moderation of terrorist

5 *Users perpetrating harm often move between platforms and services to undertake activity and disseminate content. Increasing cooperation between companies to share observations and best practice to help prevent harms spreading from one provider to another is likely to be essential to constrain this cross-platform activity.*

content and activity; and

- contribute to the development of industry expertise in tackling terrorist content and activity.

The above could be achieved through active membership of organisations such as the GIFCT, Tech Against Terrorism and TechUK, or through more informal partnerships with trusted companies.

Section 3:
User reporting

PRINCIPLE 4: Companies seek to implement effective user reporting, complaints and timely redress processes to ensure users are empowered and protected.

Context: Companies should have in place user reporting mechanisms which allow users to quickly and confidently report any concerns about terrorist content and activity which they discover when using the service. In order to minimise any infringement on users' rights to freedom of expression, where companies remove terrorist content from their services, there should be safeguards in place so that users can request reinstatement of legitimate content[6] that has inadvertently been removed.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- provide appropriate, clear and easily accessible reporting processes for users.
- have systems and processes in place to review reports from users and trusted flaggers in reporting terrorist content on their services.
- ensure there is an effective and accessible complaints function for specific concerns about terrorist content and activity.
- have appropriate appeal functions for users who have had their content inadvertently removed.
- enable users who have posted content that has been deemed to fall within the definition and scope of terrorist content and activity to appeal any decision made by the company.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- ensure there are clear and accessible reporting functions for users if they discover terrorist content and activity within a service, whilst encouraging users to contact the police if they suspect they have identified an imminent threat to life or serious physical injury.
- as far as practicable, ensure users receive timely, clear and transparent responses to their reports and are informed about decisions taken based on their report (with an appropriate level of detail, balancing transparency against national security).
- consider whether users who notify the company that they have been exposed to terrorist content and activity on a service can be directed to appropriate help and support, through collaboration with relevant civil society organisations.

6 *Content which is legal and does not breach the company's terms and conditions*

- ensure that user complaints and reporting functions are resourced to provide an effective and swift response, and that any correspondence includes appropriate coverage of user rights to challenge decisions.

The number of user reports will not in itself be seen as indicative of a service being unable to observe the principles within the code.

Section 4: Law Enforcement

PRINCIPLE 5: Companies seek to support investigation and prosecution of individuals for terrorist offences in the UK in line with existing legal frameworks and voluntary reporting measures.

Context: Companies may be the first to locate a threat or evidence that a terrorist attack is imminent or in progress. Where companies suspect that content and activity on their services involves an imminent threat to life or serious physical injury[7], and there is a clear UK nexus,[8] companies can assist UK law enforcement by reporting these offenders and retaining content for investigation and prosecution.

This gives the police the best possible opportunity to safeguard the UK public against the terrorist threat.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- prioritise removing any terrorist content and activity that breaches UK terrorism legislation, in line with Principle 1.
- comply with removal and retention requests from recognised UK law enforcement bodies e.g. the Metropolitan Police's Counter Terrorism Internet Referral Unit (CTIRU) in line with existing legal obligations.
- voluntarily report to UK law enforcement where a company suspects there is an imminent threat to life or serious physical injury related to activity occurring on their services and with a clear UK nexus, in accordance with its terms and conditions and applicable law.
- where voluntarily reporting to law enforcement, take reasonable steps to retain content and associated data, as law enforcement may request to access it for evidential purposes through existing legal mechanisms.

All reporting to authorities should be compliant with applicable legislative frameworks.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- implement automated technologies and/or human moderation that enable expeditious identification of terrorist content and activity indicating an imminent threat to life or serious physical injury, as set out in Principle 1. Detection processes will vary by service type.
- report suspected imminent threat to life or serious physical injury to UK law enforcement by calling 999 or otherwise contacting the emergency services, including reporting identifying information about the user(s) responsible. It is not an essential criteria for this threat to life to be directly related to a terrorist act, so companies should refer content and activity when they suspect that it constitutes an imminent threat to life or serious physical injury. Some companies may already

7 *A suspected imminent threat to life is where a company believe someone might be seriously injured or killed very soon – this could include the person livestreaming the footage. It is not an essential criteria for this threat to life to be directly related to a terrorist act.*

8 *For example, UK based individuals, UK nationals overseas, or UK assets or interests at home or overseas.*

have specific arrangements in place with law enforcement for reporting content, which should continue to be used.

- retain terrorist content and associated data, in line with data protection laws, that has been reported to law enforcement, along with its related metadata, for law enforcement to apply to access through existing legal mechanisms.
- make suspicious activity reports related to terrorist finance in accordance with existing legislation.
- provide appropriate training and support to staff around the requirement to support UK law enforcement.
- seek to engage with the law enforcement community to exchange insights on the changing nature of the terrorist threat in the real world and online, to develop better and holistic approaches to cooperation.

Appendix 1: Definition of terrorist content and activity

User-generated content is digital content that is produced, promoted, generated or shared by users of a service that is managed and/or owned by a third party.

Online terrorist content is any content which, by uploading it or otherwise making it available to others online, a person is committing an offence under UK terrorism laws. Terrorist content online can take many forms, including but not limited to statements, imagery (including still images and others such as GIFs), videos (both live and pre-recorded), voice recordings and documentation such as leaflets, papers and posters.

Online terrorist activity means any action taken by a person online that forms part of an offence under UK terrorism laws. Generally, it is the means and techniques by which terrorists and their supporters build community, disseminate content and communicate online for terrorist purposes, including through the exploitation of differing services and accounts.

Notes on the definition of terrorist content and activity

- Whether content and activity is terrorist in nature is often not clear-cut, and companies already make difficult decisions when moderating content and activity on their services.
- While the above definition uses criminal law to demarcate terrorist content and activity from other content and activity, this does not imply that the company must be satisfied to the criminal standard of proof that the content is illegal, in order to take action. If a company addresses content and activity on the basis that it suspects on the balance of probabilities the content and activity to be terrorist in nature, they will not have to prove beyond a reasonable doubt that the content and activity would constitute that offence.
- In line with the above definition, the list of proscribed groups is set out in Schedule 2 to the Terrorism Act 2000.
- The term 'publication' is defined in section 20 of the Terrorism Act 2006.
- Through providing this clarification we are not seeking to narrow companies' own terms and conditions, which often take a broader view of harmful terrorist related content.
- All the measures outlined in this interim code fall within existing legal frameworks and are intended to be applied on a risk-based and proportionate basis.
- Section 17 of the Terrorism Act 2006 sets out that the Act applies extra-territorially; the offences can be committed by anyone anywhere in the world.

Examples of terrorism offences

Below are some examples of what terrorist content and terrorist activity could look like online. This is not an exhaustive list. Further guidance can be found on gov.uk.

Encouragement of terrorism

- A person commits an offence if he publishes a statement likely to be understood by a reasonable person as direct or indirect encouragement or other inducement, including the glorification of commission, preparation or instigation of acts and offences, to some or all of the members of the public to whom it is published, as outlined in s1(1) of the Terrorism Act 2006.
- A person commits an offence if he invites another to provide money or other property and intends that it should be used or has reasonable cause to suspect that it may be used, for the purposes of terrorism as per s15 of the Terrorism Act 2000.
- A person commits an offence if he incites another person to commit an act of terrorism wholly or partly outside the United Kingdom and the act would, if committed in the United Kingdom, constitute an offence listed in section 59(2) of the Terrorism Act 2006.

Proscribed organisations

- A person commits an offence if he belongs to, or professes to belong to, a proscribed organisation as per s11 of the Terrorism Act 2000; Schedule 2 to the Terrorism Act 2000 provides a list of proscribed organisations.
- A person commits an offence if he expresses an opinion or belief that is supportive of a proscribed organisation and in doing so is reckless as to whether a person to whom the expression is directed will be encouraged to support a proscribed organisation, as outlined in s12 of the Terrorism Act 2000.
- A person commits an offence if he publishes an image of an item of clothing or any other article in such a way or in such circumstances as to arouse reasonable suspicion that the person is a member or supporter of a proscribed organisation as per s13 of the Terrorism Act 2000.

Acts of terrorism

- A person commits an offence if he collects or makes a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or if he accesses, by means of the internet a document or record containing information of that kind, as per s58 of the Terrorism Act 2000.
- A person commits an offence if he provides or receives or invites another to receive instruction or training in the making or use of certain weapons, including firearms and explosives as outlined in s54 of the Terrorism Act 2000.

Dissemination of terrorist publications

- A person commits an offence if he engages in conduct such as: distributing or circulating a terrorist publication, transmitting the contents of such a publication electronically or giving, selling or lending such a publication as outlined in s2 of the Terrorism Act 2006.
- A terrorist publication is defined as such if the contents are likely to be understood as encouragement or incitement of terrorism or likely to be useful in the commission or preparation of terrorism.

Appendix 2: Existing initiatives

Global Internet Forum to Counter Terrorism (GIFCT)

(www.gifct.org)- The GIFCT is leading the cross-industry response to reduce the availability of terrorist content on the internet and working to ensure there are no safe spaces for terrorists online. Its stated mission (as of December 2020) is to 'Prevent terrorists and violent extremists from exploiting digital services' and the goals of the GIFCT are to:

- empower a broad range of technology companies, independently and collectively, with processes and tools to prevent and respond to abuse of their platforms by terrorists and violent extremists;
- enable multi-stakeholder engagement around terrorist and violent extremist misuse of the internet and encourage stakeholders to meet key commitments consistent with the GIFCT mission;
- promote civil dialogue online and empower efforts to direct positive alternatives to the messages of terrorists and violent extremists;
- advance broad understanding of terrorist and violent extremist operations and their evolution, including the intersection of online and offline.

Further and up-to-date information on the GIFCT can be found at www.gifct.org.

Christchurch Call to Action

(www.christchurchcall.com)- Following the terrorist attack in Christchurch, New Zealand in March 2019, many companies signed up to the Christchurch Call to Action alongside several governments and civil society organisations from across the world.

The events of Christchurch in 2019 highlighted once again the urgent need for action and enhanced cooperation among the wide range of actors with influence over this issue, including governments, civil society, and online service providers, such as social media companies, to eliminate terrorist and violent extremist content online.

The Christchurch Call is a commitment by governments and tech companies to eliminate terrorist and violent extremist content online. It rests on the conviction that a free, open and secure internet offers extraordinary benefits to society. Respect for freedom of expression is fundamental. However, no one has the right to create and share terrorist and violent extremist content online.

The Call outlines collective, voluntary commitments from governments and online service providers intended to address the issue of terrorist and violent extremist content online and to prevent the abuse of the internet as occurred in and after the Christchurch attacks.

The UK government remains committed to the Christchurch Call to Action as a key international agreement to ensure cross-industry efforts are coordinated and robust by investing in the GIFCT and by sharing knowledge and expertise.

Voluntary Transparency Reporting Protocol (VTRP)

With the support of the Australian, New Zealand and Canadian governments, the Organisation for Economic Co-operation and Development are developing the VTRP through a multi-stakeholder consultation process. The VTRP aims to produce a tiered transparency reporting framework that can then be applied by all tech companies of varying sizes and capability to support coordinated international transparency reporting which will enable an assessment of the response, strengthen understanding of the threat and ultimately, reduce terrorist and violent extremist content online. The Interim Code of Practice on Terrorist Content and Activity Online has sought to align with the developments of this protocol where appropriate.

Appendix 3: Small and medium size enterprises (SMEs)

The principles in this code are intended to be applied on a risk-based and proportionate basis, and not all of the principles will apply to every company. Government recognises that SMEs are likely to have less capacity and resources to safeguard their services and therefore may not be able to take the same measures as large companies. However, evidence shows that terrorists exploit services of all sizes and varying functionalities and therefore we expect companies to do everything they can to identify and address terrorism, whether they are a start-up or an international corporation.

This appendix aims to provide advice on this topic and encourages SMEs to consider how services and users can best be protected using available resources.

Companies are encouraged to identify which of the principles in this code apply to them, and to use their discretion to consider which of the recommended measures they can take to meet each relevant principle.

The minimum measures outlined below propose a basic framework of measures that any company (including SMEs) might implement to meet minimum expectations under this interim code. This is not prescriptive and companies are encouraged to do as much as they can to identify and combat terrorist content and activity.

Harms and risk factors to consider

It is vital that SMEs reflect upon potential harms on their services and (as the experts on the functionality of their services) potential, practicable measures to mitigate the risks these harms create. These harms could include, but are not limited to;

- targeted radicalisation of vulnerable users by bad actors;
- sharing of terrorist content, including propaganda across media types;
- posting of URLs to terrorist content and activity hosted on a third-party service; and
- live broadcast of terrorist activity.

The following questions will help ascertain key risk aggravating factors (this is not an exhaustive list).

Do your services:

- allow users to create, promote, repost or share sentiment on any type of content?
- offer ephemeral, encrypted or self-deleting content?
- use end-to-end encryption to place user content out of reach of provider moderation systems?
- offer features that enable exchange of rich media including video (stored and livestreamed), audio, images, link sharing (including via URL shortening services), virtual reality, location sharing, and contact details on other services?
- offer user profiles that may enable real-world identification of vulnerable people?

Examples of measures that can be taken by companies of any size to mitigate potential terrorist content and activity:

- offer prominent and accessible user reporting mechanisms for content and activity that a user is concerned about and have a mechanism in place to action this swiftly, which may include fast-track responses to user reporting on the most harmful types of content, such as terrorism;
- dedicated human review of select forms of terrorist content and activity;
- gaining access to low/no-cost knowledge, practical support and tools (e.g. automated moderation and detection of terrorist content and activity) from existing cross-industry groups. For more information about safety technology companies see the Directory of UK Safety Tech Providers and the Safety Tech Innovation Network website;
- where no user reporting system is in place, signposting users to the government's online tool for reporting terrorist or extremist content (https://www.gov.uk/report-terrorism)[9];
- publication of clear and accessible terms and conditions, which should describe what the company considers to be acceptable content on their services;
- state in a clear and accessible way the sanctions for any failures to comply with terms and conditions for content and activity e.g. provider will remove identified content, suspend, close or otherwise restrict user accounts, make reports to UK law enforcement where the nature of the content causes suspicion of an imminent threat to life or serious physical injury;
- ensure services are safe by design as far as practicable (please see Part 5 in the Full Government Response); and
- apply the sanction framework in a consistent and transparent way.

9 *This is a tool designed to receive referrals of such content from the public. All referrals made go directly to the Counter Terrorism Internet Referral Unit (CTIRU) in the Metropolitan police for assessment and investigation.*