

Abhorrent Violent Conduct Powers Regulatory Guidance

eSC RG 5

December 2021



Contents

Overview of this guidance	2
Overview of the Abhorrent Violent Conduct Powers	2
Key terms	3
What is ‘abhorrent violent conduct’?	3
When would there be ‘significant harm to the Australian community’?	3
What is an ‘online crisis event’?	4
Making the decision to request or require blocking	4
Approaches to compliance and enforcement	5
Compliance and enforcement options	5
Blocking requests	5
What is a blocking request?	5
When can a blocking request be issued?	6
How long can a blocking request be in place?	6
Can a blocking request be revoked?	6
What are the consequences of ignoring a blocking request?	6
Blocking notices	7
What is a blocking notice?	7
When can a blocking notice be issued?	7
How long can a blocking notice be in place?	8
Can a blocking notice be revoked?	8
What are the penalties for ignoring a blocking notice?	8
Material that is exempt from blocking powers	9
Review rights	9

Overview of this guidance

eSafety is committed to empowering all Australians to have safer, more positive experiences online.

This information is for members of the general public, industry and other professionals who require further information about the Abhorrent Violent Conduct Powers.

It provides an overview of the actions available to eSafety under the Online Safety Act 2021 (the Act) to prevent Australian internet users from accessing material that promotes, incites, instructs in or depicts abhorrent violent conduct. These powers protect the Australian community by seeking to prevent the viral, rapid and widespread distribution online of terrorist and extreme violent material, such as the video created by the perpetrator of the March 2019 Christchurch terrorist attack.

This document explains how eSafety will generally interpret and apply the law when using our powers under the Act. All decisions will be made on a case-by-case basis.

Overview of the Abhorrent Violent Conduct Powers

The Act includes a number of powers which allow eSafety to request or require an internet service provider to block material that promotes, incites, instructs in or depicts abhorrent violent conduct.

A request is communicated by issuing blocking request, while a requirement is communicated by issuing a blocking notice.

Before issuing a blocking request or a blocking notice, eSafety must be satisfied that the availability of the material online is likely to cause significant harm to the Australian community.

There are several enforcement actions available to eSafety where an internet service provider fails to comply with a blocking notice. This includes seeking an injunction or civil penalty order for any provider that fails to block material in response to our notice.

It is intended that blocking requests and blocking notices will be issued in situations where an online crisis event has been declared by eSafety. This is not a statutory requirement, but set out in a protocol developed by eSafety, Australian internet service providers and the Communications Alliance (an industry body for the Australian communications sector). The Abhorrent Violent Conduct Powers will operate in tandem with this protocol. The protocol sets out the administrative procedures required to notify providers of a potential online crisis event, including key contacts and notification arrangements.

For further information about when eSafety may not use these powers, see [**Material that is exempt from eSafety's blocking powers on page 9.**](#)



Key terms

What is 'abhorrent violent conduct?'

Abhorrent violent conduct occurs when a person:

- engages in a terrorist act
- murders another person
- attempts to murder another person
- tortures another person
- rapes another person, or
- kidnaps another person using violence or the threat of violence.¹

The Abhorrent Violent Conduct Powers address material that:

- promotes abhorrent violent conduct
- incites abhorrent violent conduct
- instructs in abhorrent violent conduct, or
- depicts abhorrent violent conduct.

When would there be 'significant harm to the Australian community'?

In considering whether the availability of abhorrent violent conduct material online is likely to cause significant harm to the Australian community, eSafety must take into account:

- the nature of the material
- the number of internet users who are likely to access the material, and
- any other matters that eSafety considers relevant.²

eSafety may also consider the harm that is reasonably likely to result from access or exposure to that material including, but not limited to:

- trauma or terror as a result of the material
- any radicalisation or contagion effect of the material
- the use of the material to incite further terrorist acts or violent crimes
- the use of the material to seriously threaten, harass, intimidate, humiliate or abuse Australians generally, or any specific community group of Australians.

Other factors eSafety may consider include:

- whether the spread of the material is active and in progress
- how accessible the material is in Australia
- how rapidly and widely the material is being spread
- the extent and effectiveness of any efforts by the online industry to stop the spread of the material.

¹Section 474.32(1) of the Criminal Code 1995 (Cth). ²Sections 95(4) and 99(4) of the Act.

What is an 'online crisis event'?

An online crisis event can be declared when abhorrent violent conduct material is shared or spread online in a manner likely to cause significant harm to the Australian community, in circumstances warranting a rapid, coordinated and decisive response by industry and government.

eSafety receives information from law enforcement, relevant government agencies, industry and other sources, including members of the public, which may assist in determining whether circumstances should be declared as an online crisis event. Any declaration of an online crisis event is made in consultation with relevant government agencies and bodies.

Making the decision to request or require blocking

The issuing of a blocking request or blocking notice is at eSafety's discretion. This means eSafety makes the final decision about whether we will take action. Not all situations involving the spread of abhorrent violent conduct material during an online crisis event will require eSafety to take action.

Under the Act, before issuing a blocking request or a blocking notice, eSafety must consider whether any of our other powers could be used to minimise the likelihood of the material causing significant harm to the Australian community.³ eSafety may also take into account any other factors we consider relevant when deciding whether to use our blocking powers.

Depending on the circumstances, eSafety may choose to use other removal powers under the Act rather than issuing a blocking request or a blocking notice. Under the Online Content Scheme,⁴ eSafety may issue a removal notice requiring certain online service providers to remove illegal and restricted material, including material that advocates the doing of a terrorist act and material that promotes, instructs or incites in matters of crime and violence. Regulatory guidance about the Online Content Scheme can be found [here](#).

Alternatively, eSafety may choose to issue a notice relating to abhorrent violent material under the Criminal Code 1995 (Cth) (Criminal Code). These are not removal notices but are intended to make certain online service providers aware of abhorrent violent material on or hosted by the service. Guidance on these powers can be found [here](#).

There may be occasions when eSafety decides to issue a number of different notices, including removal notices under the Online Content Scheme,⁵ abhorrent violent material notices under the Criminal Code and blocking notices under the Abhorrent Violent Conduct Powers.



³Sections 95(5) and 99(5) of the Act. ⁴Part 9 of the Act. ⁵Sections 109 and 110 of the Act.

Approaches to compliance and enforcement

Compliance and enforcement options

Under the Act, eSafety may issue blocking requests⁶ and blocking notices.⁷

The two powers will ordinarily be used as part of a two staged approach designed to give industry the opportunity to take quick and voluntary action under a blocking request, before an enforceable blocking notice is issued. However, it is at the discretion of eSafety as to whether to issue a blocking request or move straight to issuing a blocking notice.

When issuing a blocking request or a blocking notice, eSafety does not have to observe any procedural fairness requirements.

Blocking requests

What is a blocking request?

A blocking request is a written notification requesting that an internet service provider take one or more specific steps to disable access to particular abhorrent violent conduct material. Internet service providers are not required to respond to a blocking request as it is voluntary. As such, there are no sanctions for non-compliance with the request.

Examples of steps that a provider could be asked to take include steps to block:

- domain names that provide access to the material
- URLs that provide access to the material
- IP addresses that provide access to the material.⁸

In most cases, eSafety will supply providers with a list of domains to block, rather than IP addresses or URLs. The intention of this is to prevent over blocking of an IP address that disables access to more than just the abhorrent violent conduct material. Material at specific URLs may also be better dealt with through more targeted interventions such as removal notices under the Online Content Scheme and abhorrent violent material notices under the Criminal Code. Where blocking at the domain level risks over blocking, eSafety will also consider use of these alternative powers.

⁶Section 95 of the Act. ⁷Section 99 of the Act. ⁸Section 95(2) of the Act.

When can a blocking request be issued?

It is intended that a blocking request will be issued in situations where an online crisis event has been declared by the eSafety Commissioner.

A blocking request can be issued where:

- the material can be accessed using an internet carriage service supplied by an internet service provider
- eSafety is satisfied that the material depicts, promotes, incites or instructs in abhorrent violent conduct, and
- eSafety is satisfied that the availability of the material online is likely to cause significant harm to the Australian community.⁹

Where an internet service provider has been requested to take steps to block a domain or related URL, and the person to whom the domain name is registered is known to eSafety, eSafety must give that person a copy of the blocking request as soon as possible after it is issued to the internet service provider. This informs the owner that the request has been made due to abhorrent violent conduct material being available on their domain.

How long can a blocking request be in place?

A blocking request remains in place for a period specified in the request, which must be no longer than 3 months.¹⁰ The request is designed to be time-limited to minimise adverse effects on blocked domains while still preventing potential harms that may result from the spread of abhorrent violent conduct material.

Under the industry protocol related to this guidance, blocking requests will normally be for five days, depending on the nature, scope and severity of the online crisis event.

If a request is about to expire but the material still needs to be blocked, eSafety can issue a new blocking request that comes into force immediately after the expiry of the original request.¹¹

Can a blocking request be revoked?

eSafety may revoke a blocking request by giving written notice to the internet service provider.¹² This would ordinarily be done if the domain or URL ceases to provide access to the abhorrent violent conduct material, or if eSafety considers enough time has passed to reduce the likelihood that the material will spread to a large number of internet users.

What are the consequences of ignoring a blocking request?

There is no enforcement action which arises from a failure to comply with a blocking request after receiving it.

When a provider complies with a blocking request, the provider will be protected from civil proceedings for anything done in compliance with that request.¹³

⁹Section 95(1) of the Act. ¹⁰Section 96(2) of the Act. ¹¹Section 96(3) of the Act. ¹²Section 97(2) of the Act. ¹³Section 221(2)(f) of the Act.

Blocking notices

What is a blocking notice?

A blocking notice is a written notice requiring an internet service provider to take one or more specific steps to disable access to abhorrent violent conduct material.

Examples of steps that a provider could be asked to take include steps to block:

- domain names that provide access to the material
- URLs that provide access to the material
- IP addresses that provide access to the material.¹⁴

In most cases, eSafety will supply providers with a list of domains to block, rather than IP addresses or URLs. The intention of this is to prevent over blocking of an IP address that disables access to more than just the abhorrent violent conduct material. Material at specific URLs may also be better dealt with through more targeted interventions such as removal notices under the Online Content Scheme and abhorrent violent material notices under the Criminal Code. Where blocking at the domain level risks over blocking, eSafety will also consider use of these alternative powers.

When can a blocking notice be issued?

It is intended that a blocking notice will be issued in situations where an online crisis event has been declared by the eSafety Commissioner.

A blocking notice can be issued where:

- the material can be accessed using an internet carriage service supplied by an internet service provider
- eSafety is satisfied that the material depicts, promotes, incites or instructs in abhorrent violent conduct, and
- eSafety is satisfied that the availability of the material online is likely to cause significant harm to the Australian community.¹⁵

There is no requirement to issue a blocking request before a blocking notice. eSafety is able to determine the best course of action according to the circumstances of the particular matter.

Where a blocking notice is issued to require an internet service provider to take steps to block a domain or related URL and the registered owner of the domain name is known to eSafety, eSafety must give that person a copy of the blocking request as soon as possible after it is issued to the internet service provider.¹⁶ This informs the owner that the request has been made due to abhorrent violent conduct material being available on their domain.



¹⁴Section 99(2) of the Act. ¹⁵Section 99(1) of the Act. ¹⁶Section 98 of the Act.

How long can a blocking notice be in place?

A blocking notice remains in place for a period specified in the notice, which must be no longer than 3 months.¹⁷ The notice is designed to be time-limited to minimise adverse effects on blocked domains while still preventing potential harms that may result from the spread of abhorrent violent conduct material.

Under the industry protocol related to this guidance, blocking notices will normally be for five days, depending on the nature, scope and severity of the online crisis event.

If a notice is about to expire but the material still needs to be blocked, eSafety can issue a new blocking notice that comes into force immediately after the expiry of the original notice.¹⁸

Can a blocking notice be revoked?

eSafety may revoke a blocking notice by giving written notice to the internet service provider.¹⁹ This would ordinarily be done if the domain or URL ceases to provide access to the abhorrent violent conduct material, or if eSafety considers enough time has passed to reduce the likelihood that the material will spread to a large number of internet users.

What are the penalties for ignoring a blocking notice?

An internet service provider must comply with a requirement under a blocking notice.

Failure to comply with a blocking notice may result in a civil penalty of up to 500 penalty units.²⁰

eSafety may also take enforcement action where an internet service provider has failed to comply with a blocking notice. Options available include the following:

- **Enforceable undertakings.** An internet service provider may enter into an agreement with eSafety to ensure compliance with the blocking notice requirements. Once accepted by eSafety, the undertaking can be enforced by the Federal Court of Australia and the Federal Circuit Court of Australia.²¹
- **Injunctions.** An injunction is an order granted by the Federal Court of Australia or the Federal Circuit Court of Australia to compel an internet service provider to take certain actions, or to refrain from taking certain actions, to comply with the blocking notice requirements.²²

When a provider complies with a blocking notice, the provider will be protected from civil proceedings for anything done in compliance with that notice.²³

¹⁷Section 96(2) of the Act. ¹⁸Section 96(3) of the Act. ¹⁹Section 97(2) of the Act. ²⁰Section 103 of the Act. The monetary value of 1 penalty unit is \$222 (until 30 June 2023) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual. ²¹Section 164(1)(j) of the Act.

²²Section 165(1)(j) of the Act. ²³Section 221(2)(g) of the Act.

Material that is exempt from blocking powers

The Act provides for circumstances where abhorrent violent conduct material is exempt from the blocking request and blocking notice provisions.

The exemptions are limited to circumstances where ongoing access to the material is:

- necessary to enforce, monitor compliance with, or investigate a contravention of an Australian law (Commonwealth, State and Territory laws) or a law of a foreign country or part of a foreign country
- for the purpose of proceedings in a court or tribunal
- necessary for conducting scientific, medical, academic or historical research, and reasonable in the circumstances for this purpose
- related to a news or current affairs report that is in the public interest and made by a person working in a professional capacity as a journalist
- connected with the performance of a public official's duties or functions (or assisting a public official in relation to those duties or functions) and is reasonable in those circumstances
- for the purpose of advocating the lawful procurement of a change to any matter of law, policy or practice established by Australian law (Commonwealth, State and Territory laws) or the law of a foreign country or part of a foreign country, or
- related to the development, performance, exhibition or distribution, in good faith, of an artistic work.²⁴

Review rights

The decision to issue a blocking notice is a reviewable decision. The decision can be reviewed internally by eSafety and externally by the Administrative Appeals Tribunal. A decision to issue a blocking request is not a reviewable decision.

²⁴Section 104 of the Act.

