How the Online Safety Act supports those most at risk online

About the Online Safety Act

The internet is an essential service that is an important part of our daily lives. It can be critical for people who depend on technology to connect to others in their community.

But as our online activity rises, so do the risks. We know from eSafety's research and investigative insights that some individuals and communities are targeted by online abuse more than others.

We also know that online risks and harms are growing and changing, so eSafety needs to change as well.

In 2015, Australia's Enhancing Online Safety Act established the Office of the Children's eSafety Commissioner. In 2017, our role was extended to protecting all Australians from online harm, not just children. Now the Online Safety Act 2021 has given eSafety wider, more effective powers to help us keep pace with changes in technology and online behaviours.

In this fact sheet:

- eSafety's approach to combating online harm
- The people who are most at risk
- How the new laws help
- How we prioritise support for those most at risk
- How we encourage tech companies to reduce abuse
- Where to find more information

eSafety's approach to combating online harm

eSafety takes a comprehensive approach to tackling online risks and harms. We have an extensive range of programs, resources and services focused on three key roles – prevention, protection and proactive change.

- **Prevention:** Our goal is to prevent online harms from happening in the first place. We do this by conducting research that identifies online risks and the most effective ways of reducing them, then running education and community programs that raise awareness and provide the skills and resources that people need to protect themselves online. Many of our programs are specially tailored for kids, young people, parents, teachers, women, diverse communities and older Australians.

- **Protection:** eSafety has a range of powers to protect Australians by directing online and electronic services and platforms to remove seriously harmful content. This can include child sexual abuse material, pro-terrorist content and intimate images shared without the consent of the person shown. Also, if the online service or platform does not help in cases

of cyberbullying of children and serious adult cyber abuse, eSafety can investigate and have the harmful content removed. Our new regulatory tools are supported by <u>Basic Online Safety Expectations</u> and will include enforceable industry codes.

- **Proactive change:** By highlighting emerging trends and challenges and providing self-assessment tools, we put the onus on tech companies to change their practices so the safety of their users is as important as their security and privacy. This includes <u>Safety by Design</u>, a proactive and preventative approach that focuses on embedding safety into the culture and leadership of tech organisations.

The people who are most at risk

Our research shows that some individuals and communities are more at-risk of being targeted online, and at-risk of serious harm, due to a range of intersectional factors. These factors include race, religion, cultural background, gender, sexual orientation, disability and/or mental health condition.

The risk can also increase because of situational vulnerabilities, such as being impacted by domestic and family violence. These are some examples of disturbing trends:

- <u>Aboriginal and Torres Strait Islander peoples</u> experience online hate speech at more than double (33%) the national average in Australia (14%).

- The same is true for <u>LGBTIQ+</u> individuals, 30% of whom experience hate speech (compared to 14% for the rest of the population).

- People from <u>culturally and linguistically diverse backgrounds</u> experience online hate speech at higher levels (18%) than the national average in Australia (14%).

- For <u>people with disability</u>, abuse disproportionately targets their disability and physical appearance.

- <u>Women</u> face disproportionate levels of online abuse. Two-thirds of eSafety's youth-based cyberbullying reports, image-based abuse reports and informal adult cyber abuse reports are made by women and girls.

How the new laws help

The new laws give all Australians stronger protections against harm – adults, as well as children.

Online and electronic services and platforms now have half the time to remove harmful content when directed by eSafety (24 hours instead of 48 hours). The laws apply to harmful content that is sent or shared in a wide range of ways, including:

- social media services

- messaging services

- email services

- chat apps

- interactive online games

- forums

- websites.

A world-first Adult Cyber Abuse Scheme

A key new power under the <u>Online Safety Act</u> is the ability to take formal action against serious adult cyber abuse. <u>Adult cyber abuse</u> is when content sent to someone or shared about them is menacing, harassing or offensive and also intended to seriously harm their physical or mental health. If the online service or platform used to send or share the harmful content does not help, eSafety can investigate and have the content removed.

The <u>Adult Cyber Abuse Scheme</u> does not specifically refer to racism or hate speech, but our investigators will consider whether a person has been targeted for abuse because of factors such as their race, religion, cultural background, gender, sexual orientation, disability and/or mental health condition.

A stronger Cyberbullying Scheme for children and young people

eSafety can now direct that seriously harmful content is removed from all online and electronic services and platforms that are popular with under 18s, not just from social media. To meet our threshold for investigation, the <u>cyberbullying</u> content must be seriously threatening, seriously intimidating, seriously harassing and/or seriously humiliating. If the online service or platform used to send or share the harmful content does not help, eSafety can have it removed.

An updated Image-Based Abuse Scheme

If someone shares, or threatens to share, an intimate image or video without the consent of the person shown, it is called '<u>image-based abuse</u>'. eSafety can now direct online services to remove this content within 24 hours. This faster removal helps stop the spread of the content and limit the harm done to the person targeted. The intimate content can show:

- a person's genital area or anal area (whether bare or covered by underwear)
- a person's breasts (if the person identifies as female, transgender or intersex)
- private activity (for example a person undressing, using the toilet, showering, bathing or engaged in sexual activity)
- a person without attire of religious or cultural significance that they would normally wear in public (such as a niqab or turban).

Image-based abuse should be reported to eSafety immediately.

Illegal online content

The Online Content Scheme gives eSafety new powers to regulate the worst types of harmful online material no matter where they are hosted. <u>Illegal online content</u> shows or encourages violent crimes including child sexual abuse, terrorist acts, murder, attempted murder, rape, torture, violent kidnapping and suicide. Illegal online content should be reported to eSafety immediately,

so we can have it removed.
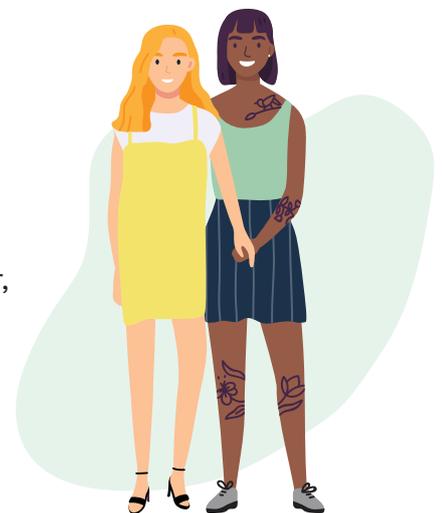
How we prioritise support for those most at risk

eSafety's public statement <u>Protecting Voices at Risk Online</u> outlines how some individuals and groups are at greater risk of being the target of online harms.

This includes groups such as <u>women</u>, <u>Aboriginal & Torres Strait Islander peoples</u>, <u>LGBTIQ+ individuals</u>, <u>people with a disability</u>, or people from a <u>culturally and linguistically diverse background</u>. The statement demonstrates how eSafety prioritises our resources and education programs to protect and build the capacity of people most at risk.

eSafety works with communities across Australia to better understand their online experiences. We work with them to deliver support programs and to help drive behavioural change.

In addition, eSafety delivers primary prevention programs that support parents and educators to teach children about cyberbullying, respectful online relationships, online consent, building good online habits and having open communication about online safety. This is part of a broader effort to prevent online harm, promote the positive potential of technology and contribute to efforts to achieve equality for people most at risk of abuse.

How we encourage tech companies to reduce abuse

<u>Safety by Design</u> is an eSafety initiative that encourages technology companies to anticipate, detect and eliminate online risks. This is one of the most effective ways to make our digital environments safer and more inclusive, which is especially important for people at greater risk of harm.

Best practice sees some online service providers using technologies to detect and remove harmful online content before it reaches the person targeted or is shared on a public platform.

These are some specific steps we recommend companies adopt:

- Explicitly reference approaches to racial abuse in internal policies and procedures and embed clear escalation paths to law enforcement and support services into the design and architecture of services and products.

- Engage people with diverse backgrounds and experiences throughout the product development and product review lifecycle so that features and functions are developed with their specific needs in mind.

- Make reporting or complaint features and functions easy to find and simple to use.

- Provide users with tools to regulate and control their own online experiences. This includes the ability to ignore, mute or block activity from specific accounts, and to exclude specific words or phrases to minimise exposure to targeted and persistent abuse while still preserving evidence of it.

(i) Where to find more information

<u>Read about</u> eSafety's regulatory philosophy and priorities , and check our regulatory guidance.