



eSafety

CORPORATE PLAN

2022-2023



esafety.gov.au



Acknowledgement of Country

eSafety acknowledges the Traditional Custodians of Country throughout Australia and their continuing connection to land, waters and community. We pay our respects to Aboriginal and Torres Strait Islander cultures, and to Elders past, present and emerging.

Contents

<u>From the Commissioner</u>	1
<u>About us</u>	3
<u>Our key activities</u>	5
<u>Our strategic priorities</u>	6
<u>Our environment</u>	8
<u>Capability</u>	12
<u>Risk management</u>	15
<u>Performance measures</u>	21

From the Commissioner



eSafety's work touches the lives of almost every Australian – and that is because almost every Australian has been touched by technology, for better or worse.

eSafety leads, co-ordinates and advises on safety issues to make sure everyone can enjoy safer and more positive experiences online. We are the first online harms regulator in the world to take on such a momentous task and have had seven years of runway to achieve an effective operating model that is delivering results.

This inaugural eSafety corporate plan gives the Australian Government, the public and all our stakeholders an understanding of our purpose and objectives. It details our functions and our roles. It outlines what we will do to achieve our purpose. And it explains how we will measure our performance.

We have prepared this corporate plan for the 2022-23 reporting year and to cover the reporting periods 2022-23 to 2025-26.

As a living document, we will update our plan every year, and we will report on the key performance indicators in this plan through the annual performance statement in our annual report.

Just as technology never stays still, neither will we, so we expect that we will need to pivot, innovate and evolve our operations to meet emerging threats.

Our corporate plan – and the annual planning process that produces it – are central to our ability to set measurable performance targets.

We are seeking to measure what matters. Much of what eSafety does is qualitative – and some of the harm remediation support we provide is incalculable.

Regulating the internet for online harms is a novel, expansive and challenging task. With almost all of our regulatory targets domiciled overseas, threat vectors changing constantly, and the identities of the perpetrators behind the harms often obfuscated and jurisdiction questioned, we face a complex range of performance challenges in terms of enforcement.

The development of our first corporate plan is an important milestone for eSafety and I want to thank all the staff who helped to develop these measures – measures that reflect the work we do to remediate harm and help Australians have safer, more positive experiences online.

As our functions are enhanced and our maturity as an organisation grows, we anticipate these performance measures will evolve in both precision and sophistication in subsequent years.

In an ever-changing world, we've got to make sure we not only keep pace, but we're also anticipating what's next. We need to recognise how the world is changing and how our operational environment needs to evolve with it. Whether that change is driven by advances in technology, changes to government policies or shifts in human behaviour and malfeasance, we need to be at the forefront of these challenges.

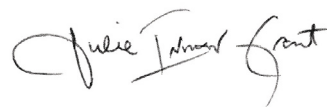
At eSafety, our vision is a world where Australians are supported and empowered to engage more safely online, and where industry around the world is enabled to lift safety standards and better meet legislated safety expectations.

This is how we plan to achieve our vision:

- **Prevent** harms from happening through evidence-based research, education programs and raising awareness
- Offer empathetic and compassionate support to **protect** people from online harms through our regulatory schemes and investigations
- Drive for **proactive** and systemic change by staying ahead of technology trends, encouraging industry to improve user safety, and strengthening our impact across international borders.
- Develop **partnerships** to amplify our reach within Australia and around the world.

In 12 months' time – when we talk again about what we will do to continue to help safeguard Australians at risk from online harms and to promote safer online experiences – I'm confident we will be able to show even more progress.

I am pleased to share our eSafety corporate plan, which signals important markers in the online safety landscape that will guide our work for years to come.



Julie Inman Grant
eSafety Commissioner

About us



About the eSafety Commissioner

The eSafety Commissioner (eSafety) is Australia's independent regulator for online safety. We foster online safety by exercising our powers under Australian Government legislation, primarily the *Online Safety Act 2021* (the Online Safety Act), to protect Australians from serious online harms.

Online harms are actions that take place wholly, or partially, online that can damage an individual's social, emotional, psychological, financial or even physical safety. These harms can occur because of content, conduct, or contact.

The Online Safety Act, the first of its kind globally, governs the functions of eSafety and includes a world-leading initiative – the Basic Online Safety Expectations determination – as well as the requirement for industry to develop new codes to regulate illegal and restricted content. The Online Safety Act also includes four reporting schemes (the Adult Cyber Abuse Scheme, the Cyberbullying Scheme for children, the Image-Based Abuse Scheme and the Online Content Scheme for illegal and restricted content) and gives eSafety powers to limit access to abhorrent violent conduct and child sexual exploitation content via search engines and apps.

eSafety does not formally require a corporate plan under the Online Safety Act given it is supported by the Australian Communications and Media Authority (ACMA). However, in light of eSafety's unique statutory remit there is significant governance and operational benefit to preparing a corporate plan. This corporate plan should be considered complementary to the [ACMA's corporate plan](#).



Purpose

To help safeguard Australians at risk from online harms and to promote safer, more positive online experiences.

Vision

Through prevention, protection and proactive and systemic change, Australians are supported and empowered to engage more safely online, and globally industry is enabled to meet legislated safety expectations.

Values

Innovation – challenging the status quo and doing things differently to lead the world to a safer online environment.

Empowerment – providing skills and knowledge to Australians so they have positive online interactions and know what to do when they encounter online harm or feel unsafe online.

Compassion – supporting Australians through difficult online experiences, providing help in an inclusive, empathetic and respectful way.

Fairness – approaching our work ethically and transparently, in a considered, fair and proportionate manner, informed by evidence and research.

Collaboration – genuinely connecting with partner organisations and industry bodies, cooperating, and sharing information, insights and expertise.

Excellence – providing online safety leadership on behalf of the Australian Government, ensuring we always have the Australian people in mind when improving and delivering our regulatory services and functions.

Our key activities

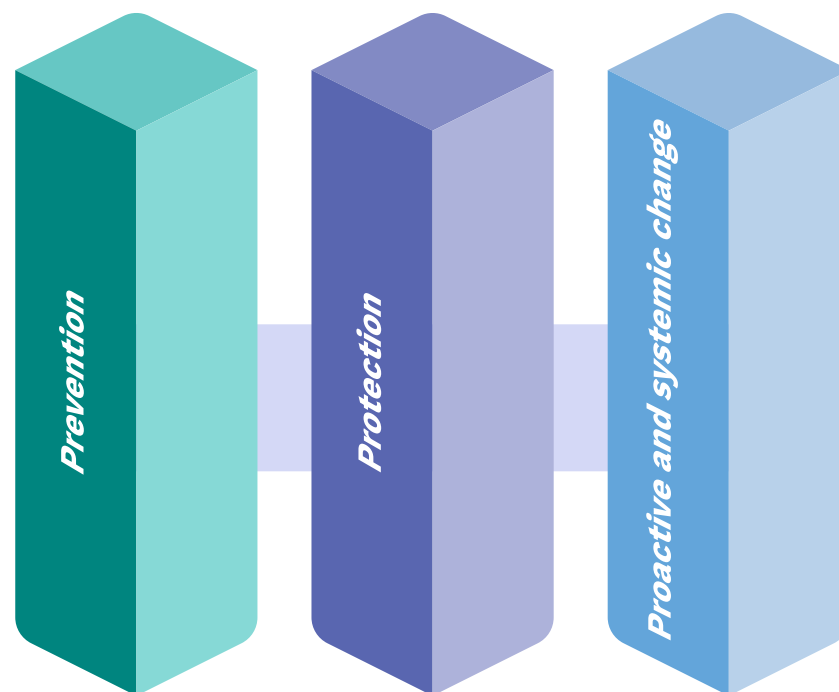


We achieve our purpose through three key pillars

Prevention: Using a solid evidence base, eSafety designs and delivers educational materials to prevent online harms, working with key sectors and community members to build user capability and resilience through training programs, awareness raising and referrals.

Protection: eSafety remediates online harms through our investigations and regulatory schemes, working with industry to build accountability and compliance in response to reported and identified harms.

Promoting proactive and systemic change: eSafety promotes proactive and systemic change, working with online industries, users, educators, governments and their agencies to reduce the threat surface for online harms, lift overall standards of online safety across industry and deliver more positive online experiences for Australians.



Our strategic priorities



The statutory functions set out under section 27 of the Online Safety Act determine the strategic priorities of the eSafety Commissioner to:

- Promote online safety for Australians
 - Provide information to Australians on the services we provide.
 - Provide and distribute information to Australians and our partners on critical online safety issues and trends.
- Administer statutory schemes to respond to complaints and conduct regulatory investigations into child cyberbullying material, adult cyber abuse material, image-based abuse, and illegal and restricted online content.
- Make sure social media services, messaging services, gaming services, file-sharing services, and other app providers and sites accessible from Australia take reasonable steps to keep Australians safe online through a set of Basic Online Safety Expectations.
- Register mandatory industry codes requiring eight sectors of the digital industry to regulate harmful online content, such as videos depicting the sexual abuse of children or terrorism, through to material which is inappropriate for children, such as online pornography.
- Coordinate the activities of Australian Government departments, authorities and agencies relating to online safety for Australians.
- Make financial grants on behalf of the Australian Government to foster online safety for Australians
- Conduct and evaluate research about online safety for Australians.

Further information on our strategic priorities can be found in Australia's [eSafety Strategy 2022-2025](#).

Corporate planning framework

The environment The global, domestic, technical, regulatory and fiscal factors that affect our work.	Purpose To help safeguard Australians at risk from online harms and to promote safer, more positive online experiences.		
	Vision Through prevention, protection and proactive and systemic change, Australians are supported and empowered to engage more safely online, and globally industry is enabled to meet legislated safety expectations.		
	Key activity 1 - Prevention Using a solid evidence base, eSafety designs and delivers educational materials to prevent online harms, working with key sectors and community members to build user capability and resilience through training programs, awareness raising and referrals.	Key activity 2 - Protection eSafety remediates online harms through our investigations and regulatory schemes, working with industry to build accountability and compliance in response to reported and identified harms.	Key activity 3 - Proactive and systemic change eSafety promotes proactive and systemic change, working with online industries, users, educators, governments and their agencies to reduce the threat surface for online harms, lift overall standards of online safety across industry and deliver more positive online experiences for Australians.
	Capabilities Activities that enable us to deliver on our mission		



Our environment



The past few years have seen an enormous shift to online learning, working, communicating, socialising and accessing services, in large part precipitated by the COVID-19 pandemic.

Consequently, millions of Australians have been exposed to increased risk of online harms. We saw evidence of this through a significant surge of reports to eSafety over periods of lockdown. This surge has settled into a ‘new normal’, with harms now being reported to eSafety at a considerably higher volume than prior to COVID-19 lockdowns.

Advances in technologies, such as machine learning, artificial intelligence and immersive technologies will continue to escalate online learning, working, and connecting, which bring the prospect of new possibilities for abuse.

eSafety has a responsibility to keep Australians safe from online abuse and illegal and restricted content. However, the online harms facing Australians are not limited to these dangers.

Several Australian Government agencies have responsibility for regulating the activities of digital businesses and protecting users. Coordination, cooperation and collaboration with our partners across government and industry is crucial as we seek to counter online harms and promote online safety.

We are closely monitoring how our environment is evolving and shaping our operating context to 2026 and beyond and we have developed this corporate plan in the context of these factors.

Global environment

As the world’s first government body dedicated to keeping people safe online, eSafety is a global leader in countering online harms and promoting online safety. We operate in a complex, rapidly changing and interconnected technological world.

Many of the businesses regulated by the Online Safety Act are domiciled offshore and are large, multinational companies. With limited domestic control and an inherent ‘power imbalance’, this adds complexity to how we engage with them and manage bilateral relationships.

Regulatory bodies in other jurisdictions are developing rapidly, with some taking a different approach to eSafety’s systemic and citizen-based model. To prevent a fragmented international regulatory environment that will impede proactive change and regulatory impact, we will continue to work with like-minded governments and their regulatory agencies to make global online safety regulation coherent, proportionate and effective.

Tech environment

The tech industry is constantly evolving. New technologies emerge, and the ways in which we use existing technologies change. We are harnessing our data to better understand how online services and platforms are being misused, conducting research and scanning the horizon for rapidly emerging technologies to anticipate and remediate potential harm, while also harnessing opportunities for technology to promote safety. Our position papers on some of these technologies can be found at [Tech trends and challenges | eSafety Commissioner](#). Areas of focus for this reporting period include:

Algorithms and machine learning

Online services can use algorithms and machine learning to reduce online harms, for example, by helping them to detect and filter out seriously harmful content at scale. However, algorithms and the broader systems in which they operate also have the potential to contribute to online harms, especially where there is a lack of transparency and accountability.

Anonymity and identity shielding

There are many ways a person can shield their identity online, and there are many legitimate safety and privacy reasons for doing so. However, real or perceived anonymity may contribute to a person's willingness and ability to abuse others online and may hinder efforts to identify and hold them responsible.

End-to-end encryption

There are many ways to encrypt information to promote privacy and security. End-to-end encryption is a specific method which is increasingly being used to secure communications from one device

or end point to another. Because the online services that offer end-to-end encryption are unable to see the content their users share, this can create opportunities for serious forms of online harm, such as the sharing of child sexual exploitation material, to go undetected.

Age assurance

Children and young people are at higher risk of a range of online safety issues. The burden for keeping them safe should rest primarily with industry rather than with parents, carers, and children and young people themselves. There is an array of existing and emerging age assurance methods which online services can employ – while protecting privacy and promoting inclusivity – to ascertain which of their users are young and then put in place appropriate safeguards.

Immersive environments and Web 3.0 / A new internet

The next iteration of the internet is potentially an immersive, enduring environment some refer to as the 'metaverse'. It is expected to be a digital world facilitated by advancements in virtual and augmented reality. There is also speculation that the next version of the internet may be decentralised, with control far more widely distributed than it is today. These developments have the potential to improve some of the current problems with safety, privacy, competition and inclusivity. However, if safety and good governance are not designed in at the start, these developments also have the potential to exacerbate existing harms, for example, through hyper-realistic experiences involving violence or abuse.

Fiscal environment

The 2022-23 Portfolio Budget Statements provides eSafety with funding of \$51.161m and an average staffing level cap of 138 to meet its current obligations.

Regulatory environment

There are several government reviews or reforms underway which will have an impact on our environment over the coming reporting cycle.

The Online Safety Act represents the most significant factor influencing the ongoing work of eSafety as the associated new regulatory schemes and provisions are enlivened.

The government's response to the House Select Committee's Inquiry into Social Media and Online Safety may consider further potential reforms and initiatives. The recommendations from that inquiry identify the need for further scrutiny, for improving Australians' access to eSafety reporting schemes and for responding to emerging technology issues.

More broadly, there are several different areas of potential regulatory reform, targeted at concerns arising in the online environment, which may impact on eSafety and its work. These include the Defamation Review and the proposed development of model defamation provisions; the review of the *Privacy Act 1988* and the potential introduction of Online Privacy Codes; potential proposals from the Australian Competition and Consumer Commission (ACCC) for digital platform-specific regulation to address competition and consumer concerns; and the review of the Digital Industry Group Inc (DIGI) disinformation code and any policy reforms arising out of the Digital Technology Task Force.

To support a streamlined and cohesive approach to the regulation of digital platforms, eSafety has joined forces with the ACMA, the ACCC and the Office of the Australian Information Commissioner (OAIC), to form the Digital Platform Regulators Forum. This initiative of Australia's independent regulators will provide a more formalised way to collaborate and share information about cross-cutting issues and activities around the end-to-end regulation of digital platforms.

Industry codes

The industry codes regime is a co-regulatory measure. We consider close collaboration between ourselves and the relevant industry associations critical to its success, as it seeks to raise the safety standards across the technology sector. During the development of the industry codes, we are working closely with an industry steering group led by the DIGI, the Comms Alliance, the Australian Mobile Telecommunications Association, the Interactive Games and Entertainment Association, the Software Alliance and the Consumer Equipment Suppliers Association. While the industry codes will be developed by industry associations with industry participants, the collaboration we provide in the form of industry workshops and feedback on draft commitments will help make sure the industry codes meet appropriate community safeguards as well as contain achievable and practical commitments.

Our response in this evolving environment

Prevention

Through research, education, and training programs, eSafety works to set a foundation to prevent online harm from happening in the first instance. We aim to provide Australians with the practical skills and confidence to be safe, resilient, and positive users of the online world, and to know where to seek help when issues do arise.

Protection

We support people experiencing online harms by compelling the removal of abusive and harmful content, limiting the ability of perpetrators to continue their abuse, and taking enforcement action against those platforms and service providers who fail to comply with regulatory notices.

Proactive and systemic change

The Online Safety Act introduced two crucial elements to improve tech safety standards, assist in mitigating some of the harms, target failed systems and processes, and bring greater accountability to the providers of online services.

The Basic Online Safety Expectations focus on making sure providers of social media services, messaging services, gaming services, file-sharing services, and other apps and certain other sites accessible from Australia, take reasonable steps to keep Australians safe online. Further information can be found at [Basic Online Safety Expectations | eSafety Commissioner](#).

The new industry codes will address issues set out in the legislation, including the proactive detection and removal of illegal content such as child sexual abuse material, while also putting a greater onus on industry to shield children from pornography and other harmful content. Further information on the development of the codes can be found at [Industry codes position paper | eSafety Commissioner](#). If the industry codes are not deemed to provide appropriate community safeguards, the eSafety Commissioner has the ability to determine industry standards for each of the eight industry sections identified in the Online Safety Act.

To further protect children from harmful online content, we are developing an age verification implementation roadmap for online pornography as requested by the Australian Government in response to a parliamentary inquiry into this issue.



Workforce capability

Since 2020, we have seen a rapid expansion in eSafety's legislative responsibilities, scope of influence, and variety of functions as a result of the Online Safety Act and several successful new policy proposals. Subsequently, there has been a commensurate increase in the size of our workforce, more than doubling in the past year. To appropriately manage and integrate our increased workforce, it has been necessary to invest in enhanced corporate systems and processes to build our organisational maturity. For the duration of this plan, we will continue to embed and further develop our corporate processes so that our operations are efficient and aligned with *Delivering for Tomorrow: the APS Workforce Strategy 2025* to deliver the best results for the Australian people.

The rate of technological change is rapid, so it is imperative our staff have the necessary skills and knowledge to adapt. To remain a relevant and modern regulator, we must be able to access the technological skills necessary to hold emergent platforms to account. We will develop an organisational capability strategy that will seek to address this challenge.

Workforce planning

There is both opportunity and need to mature our operational workforce planning, talent management and succession planning to make sure we have the diversity of thought, knowledge, agility and capability to deliver eSafety's strategic and operational objectives

now and into the future. Over the duration of this plan, we will invest in our reporting and analytical frameworks to make sure we have the right information to manage our people and sustain our workforce productivity.

eSafety's staff are employed under the ACMA Enterprise Agreement. They are employees of the ACMA but work for the eSafety Commissioner, an independent statutory office holder.

Diversity and inclusion

It is important our workforce reflects the composition of modern-day Australia so we can best serve all Australians. We have built a diverse workforce and invest significant resources in making sure we remain relevant to all Australians. The skills and experience of our people are in high demand across private industry and government, so we must continue to attract, develop and retain a diverse and highly-skilled workforce. We are committed to fostering an inclusive workplace that champions difference and harnesses the advantages of diversity. We will support and contribute to the ACMA reconciliation plan and objectives, utilise affirmative measures recruitment whenever appropriate and comply with the principles of the various APS diversity and inclusion strategies.

Learning and development

We will develop an organisational culture of continual learning and skills transfer that supports our people to successfully deliver on our strategic priorities, that drives high performance, and that builds individual and organisational capability. We will continue to leverage training opportunities where we can, accessing relevant foundational Australian Public Service (APS) offerings within the ACMA training program and the APS Academy. Given our unique profile and the technological complexity of our regulatory sphere, we will also need to harness expertise from the technology, academic and non-government organisation (NGO) communities.

Wellbeing

We prioritise employee health and wellbeing, providing information, advice, and safe and healthy work environments for our employees. The COVID-19 pandemic highlighted the importance of staff emotional and physical wellbeing to our business objectives and productivity. A firm commitment to staff wellbeing has allowed us to exceed our strategic objectives in this difficult operating environment. For the duration of this plan, we will continue to support staff wellbeing through the implementation of flexible and modern work practices, mature risk monitoring systems, and dedicated programs. We will implement recommendations contained within a comprehensive psychosocial hazard plan commissioned by the eSafety Commissioner, to address the risk to our staff from psychosocial hazards, including burnout, vicarious trauma and adverse social effects brought about through the emotionally demanding nature of our investigative work.



Technology and digital capability

Our technology and digital capability underpin all the work of eSafety and is a key enabler in helping us achieve our purpose and objectives. Our technology strategy and roadmap outlines the work underway to equip eSafety with the ICT, digital and data systems we need to deliver on our regulatory functions and strategic priorities. In 2022-23 we will develop a new three-year ICT strategy and roadmap to align with eSafety's future funding position, *Australia's eSafety Strategy 2022-25* and this plan. This is so we can continue to design and build scalable, flexible, and secure technologies to support a rapidly growing organisation.

Over the duration of this plan, we will continue to invest in the following key programs of work:

Develop regulatory and investigations technologies

We will continue to develop our complaints and investigations systems, enhancing them to support eSafety's expanded regulatory remit and improving their performance to maintain investigator wellbeing by limiting unnecessary exposure to harmful online content. This work also includes developing tools to help with rapid removal outcomes for victims of online harms, and information systems to support the Basic Online Safety Expectations and industry codes.

Enable eSafety as a data driven organisation

Our data and information management roadmap will enhance our data governance and analytics capability to support data-driven decision making, regulatory prioritisation and transparency. We will also implement a new, fit-for-purpose information management solution to make sure our record keeping capabilities remain in line with Australian Government information management standards.

Enhance core ICT delivery and cyber security capability

We will continue to modernise our ICT platforms and business systems through a cloud-first approach to new applications and technologies, maintaining priority focus on cyber protection activities including alignment with the essential eight maturity model and Protective Security Policy Framework objectives. In parallel we will continue to mature and enhance ICT governance initiatives to optimise our technology investments and stay aligned to a rapidly evolving organisation through our ICT project management office, architecture practice and change review committees.

Optimise public-facing digital products, resources, and services

We will continue to optimise and build on our award-winning digital products, resources and services to deliver best practice online safety guidance to all audiences through a variety of channels. By using best practice Web Content Accessibility Guidelines, user-centred design principles and the Digital Transformation Agency Digital Services Standard, we will continue to work to make sure all Australians have easy access to online safety materials and reporting channels.

Risk management



eSafety's risk management culture

Effective risk management contributes to improved performance and sound governance and supports good business decision making. We support our risk management culture through active engagement with risk, good governance, risk awareness and training.

Risk management framework

eSafety utilises the ACMA risk management policy and guide to provide broad policy direction and guidance to our staff. The ACMA risk management policy and guide aligns with the ISO 31000:2018 Risk Management – Guidelines, the requirements of the *Public Governance, Performance and Accountability Act 2013* and the Commonwealth Risk Management Policy, including oversight from the ACMA Audit and Risk Committee and the eSafety Risk and Compliance Committee. Our risk management processes articulate our objectives, recognise compliance requirements, identify potential opportunities, consider what may go wrong and look to prioritise, mitigate and manage risks.

Regulatory risks

The Regulatory Action Committee (RAC) supports the eSafety Commissioner in responding to emerging significant or potentially significant online harm and novel circumstances falling within the scope of our regulatory schemes. It also supports the assessment of regulatory priorities over the planning cycle.

The RAC meets regularly and advises the eSafety Commissioner about regulatory responses to novel online harms, including assessing their efficacy and impact, to support decision making. It safeguards consistency and objectivity by setting clear guidelines, and ensures proportionality by determining the nature, relativity and impact of the online harms escalated for its consideration. The focus of the RAC is on matters of widespread impact or high complexity, and strategic significance, including initial instances of online harms or where eSafety's legislative powers are deployed for the first time.

The RAC will pay close attention to all relevant data to enable ongoing monitoring of regulatory performance with a view to responding by making changes to policy or procedures should this be necessary.

eSafety's key risks

Key risks	Management response
Australians suffer from online harms	Complaints-based schemes for Australians experiencing online harms with clear regulatory guidance on their operation – Referral to appropriate support services – Education resources and programs to support all Australians including professional educators, parents, young people and women – International engagement – Basic Online Safety Expectations, Safety by Design and industry codes
eSafety has insufficient resources to meet increasing regulatory responsibilities	Regular engagement between eSafety and the Minister for Communications – Senior Executive Group oversight – Program/project management discipline applied – Best practice for regulators – Australian Government planning, reporting and transparency requirements – Deployment of additional operational resources, as required
eSafety is unable to maintain effective stakeholder relationships	Executing on our formal coordination responsibilities and stakeholder groups – Regular meetings between eSafety and the Minister for Communications – Stakeholder engagement in key sectors such as education, mental health, domestic and family violence and key community organisations – Building industry, community and internal capability – Improving data collection and analysis to assess impacts – Relationship management and coordination process and systems
eSafety is unable to effectively respond to emerging trends and global developments	Research and evaluation programs – Global connections through various forums providing thought leadership and learning from evolving regulation frameworks – Stakeholder engagement in key sectors such as education, domestic and family violence and key community organisations – Use of flexible individual contracts to procure specialist talent and build internal capacity
eSafety staff are hurt while carrying out their duties	Workplace Health and Safety policies, training and governance established and maintained – Protocols enforced to prevent or minimise psycho-social harm or vicarious trauma – Business continuity management – COVID-19 safe workplace arrangements
eSafety resources are not used effectively	Australian Government planning, reporting and transparency requirements – Regular meetings between eSafety and the Minister for Communications – System of risk management and internal control – Internal audit program and independent Audit and Risk Committee
Our communication and information assets are compromised	System of risk management and internal control – Protective security, data breach and disaster recovery arrangements – Business continuity management – Privacy management arrangements

Cooperation

We operate in a multifaceted ecosystem populated by a wide spectrum of stakeholders, including young people, parents, carers, the technology industry, law enforcement agencies, the education sector, mental health services, non-government organisations and a diverse range of domestic and international regulators. None of us will achieve our desired impact without cooperation, collaboration and partnership.

eSafety builds and nurtures partnerships and collaborations at local, state, national and global levels and across many sectors of the economy. As a small organisation, we invest strategically in partnerships with a shared vision that helps us achieve our joint goals, at scale.

We engage in a variety of ways, such as working with NGOs and other providers to promote best practice education, serving on boards and government forums, sponsoring research, and collaborating on joint educational campaigns or through operational partnerships.

ACMA

The ACMA provides corporate support services and staff to fulfil the functions of eSafety under section 184 of the Online Safety Act. The effective provision of these support services is critical to our ability to fulfil our purpose and deliver results.



Collaboration and cooperation - case studies



Partnering for online safety education

eSafety works with partner organisations to increase access to quality online safety education around Australia and to help meet the needs of diverse cohorts and communities. Through the Trusted eSafety Provider program, eSafety endorses providers of online safety education that demonstrate appropriate expertise and experience and works with them to share the latest information and to support best-practice approaches. In 2020–21, these providers reached more than 750,000 participants, including students, teachers and parents. Under the Online Safety Grants Program, eSafety provides grants to NGOs to deliver innovative projects and targeted online safety education for diverse audiences, including children in First Nations, culturally and linguistically diverse (CALD) and LGBTQI+ communities, and those living with disabilities or in out-of-home care.

The Australian Football League

eSafety and the AFL have joined forces to tackle the important issue of online safety within and outside the AFL community. Together, we want to send a strong message to players, fans and the wider community: we all need to play it safe and fair online. As part of the agreement, the AFL will continue to support eSafety's #PlayitFairOnline campaign to help educate players, fans and the community on how they can combat online abuse and protect others online.

eSafety will also provide online safety training to the AFL and its clubs and advise on best practice approaches to keeping people safe online. The agreement strengthens our ongoing partnership and will support the AFL in continuing to promote online safety through its channels to the broader Australian community and staying up to date with latest developments in the industry. The partnership has also seen the release of a set of easy-to-follow guidelines developed by eSafety to encourage players and fans to be respectful online.

The Online Safety Youth Advisory Council

eSafety has appointed 24 young people aged 13 to 24 from across Australia to our first Online Safety Youth Advisory Council to help shape our responses to online safety challenges and co-create policies and programs that will resonate with and reach other young people, and ultimately shape behaviour change. The Council is an opportunity for young people to be a voice to government about their online experiences and how these can be safe and positive. Members of the Council are from a diverse range of experiences, genders, cultural and linguistic backgrounds, and locations, and will be supported by eSafety staff.



Collaboration and cooperation - case studies

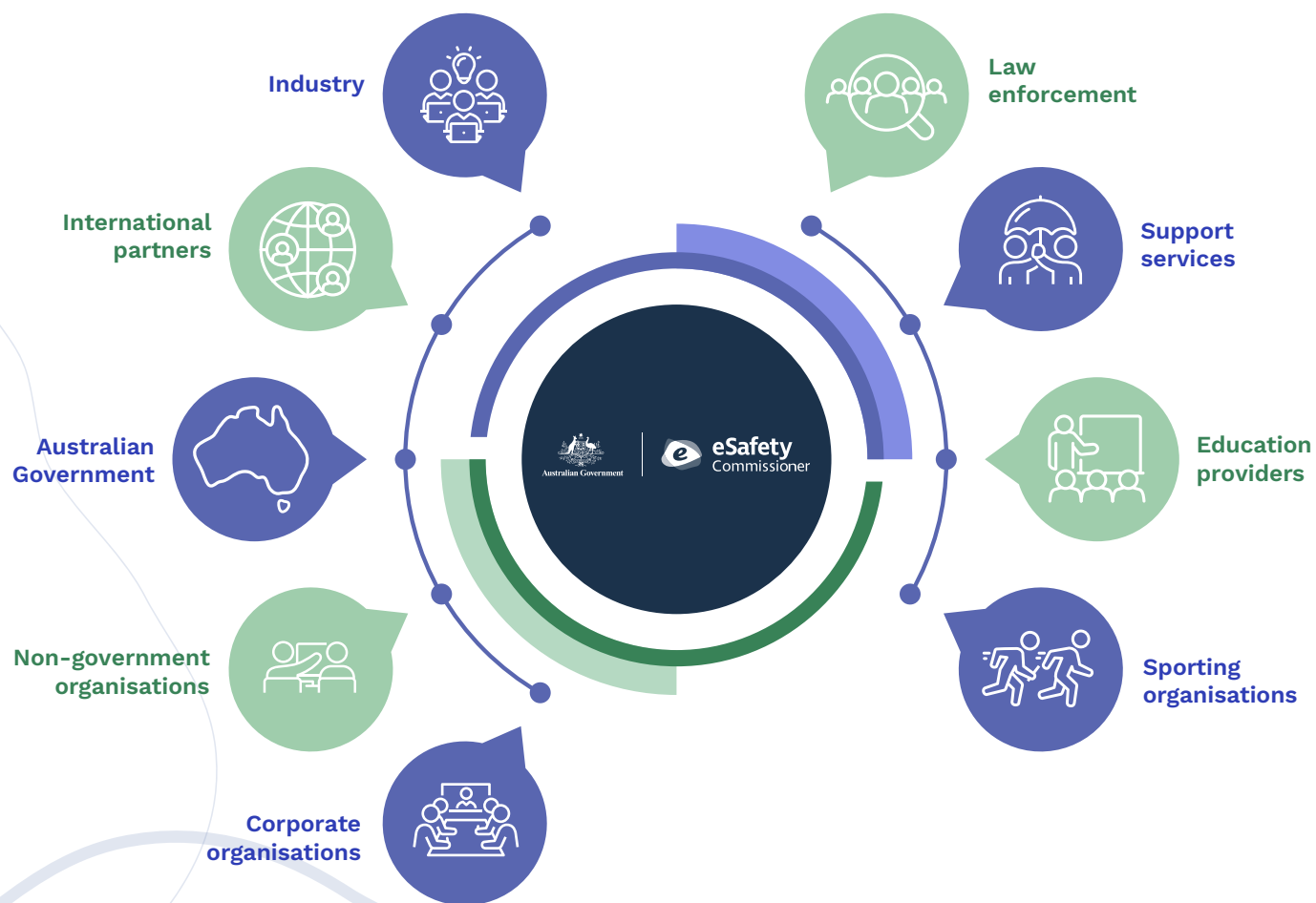
The Global Partnership for Action on Gender Based Online Harassment and Abuse

eSafety represents Australia as a member of the Global Partnership for Action on Gender Based Online Harassment and Abuse, an expanding coalition of six countries, led by the United States and Denmark. The Global Partnership works to better prioritise, understand, prevent, and address the growing scourge of technology-facilitated gender-based violence. Through the Global Partnership, we share Australia's best-practice programs and research to advance global responses to technology-facilitated gender-based violence to further share our experiences, tools and influences across the globe.

Regional capacity building

eSafety builds the capacity and capability of online safety regulators and services across the Pacific and South-East Asia (funded under the Department of Foreign Affairs and Trade's Cyber and Critical Tech Program). Taking a partnership approach, we work to contextualise and extend our world-leading online safety model for operation. We also support the development of training resources and awareness sessions for frontline women's services to increase the prevention and identification of online gender-based violence and technology-facilitated abuse.

Our stakeholders and partners



Industry: social media platforms, industry bodies

International partners: INHOPE, WeProtect Global Alliance, Global Partnership for Action on Gender Based Online Harassment and Abuse, Canadian Centre for Child Protection

Australian Government: National Office for Child Safety, Australian Human Rights Commission, Australian Curriculum, Assessment and Reporting Authority and Department of Education

Non-government organisations: Trusted eSafety Providers, grant recipients, Good Things Foundation, Australia's National Research Organisation for Women's Safety and Universities Australia

Corporate organisations: Telstra, Optus, Australian Banking Association, Qantas, Woolworths, NBN and Australia Post

Law enforcement: Australian Federal Police, state law enforcement agencies, Australian Centre to Counter Child Exploitation, Crime Stoppers NSW, Australian Institute of Criminology and AUSTRAC

Support services: Kids Helpline, Parentline, Headspace, Beyond Blue, Butterfly Foundation, Lifeline and Reachout

Education providers: Schools, early learning services, university sector and teacher accreditation organisations

Sporting organisations: Sports associations such as the AFL, Sports Integrity Australia, Australian Athletes Alliance, Sport Australia, Paralympics Australia and Disability Sports Australia

Performance measures



Key activity 1

Using a solid evidence base, eSafety designs and delivers educational materials to prevent online harms, working with key sectors and community members to build user capability and resilience through training programs, awareness raising and referrals.

Performance area 1.1: Educating Australians

Intended result: Australians are enabled by education, training and resources to prevent online harms.				
Performance measure	Targets			
	2022-23	2023-24	2024-25	2025-26
1.1.1 Number of participants in front-line and professional learning training sessions.	8,500	Increase from previous year		
1.1.2 Number of unique visitors to eSafety websites.	1.4m	Increase from previous year		
1.1.3 Proportion of Be Connected learners satisfied with training courses.	≥ 90%	Maintain		

Rationale:
By undertaking research, delivering education and training programs and producing online resources, we work to set a foundation to prevent online harm from happening. We work with our prevention partners, such as community groups, educators, law enforcement agencies and Trusted eSafety Providers, to expand awareness and extend the reach of our online safety messages and services.

Methodology:
1.1.1 The number of participants is recorded in each session. Professional learning sessions include those delivered to teachers, pre-service teachers, mental health and wellbeing professionals and family and domestic violence workers.
1.1.2 Website data collating unique visitors, including Be Connected.
1.1.3 Learner satisfaction rating is an average of responses to four questions. Satisfaction is recorded when learners agree or strongly agree that the material is 'well organised and easy to follow', 'the content is relevant to me', 'the material is interesting and engaging' and that they 'feel inspired or confident to practice the skills covered'.

PBS links:
Program 1.3 – Office of the eSafety Commissioner
 Support positive online experiences through national leadership and administration of statutory schemes and educational and awareness activities that promote online safety for all Australians.
 - Promote online safety for all Australians

Performance area 1.2: Understanding of needs

Intended result: Educational programs, strategies and tools are based on an understanding of the specific needs of groups most at risk of online harm.				
Performance measure	Targets			
	2022-23	2023-24	2024-25	2025-26
1.2.1 Proportion of resources informed by research and insights and involve co-design or collaboration with targeted cohorts and/or advocates.	100%	Maintain		
1.2.2 Publication of eSafety online harms threat assessment.	Inaugural publication	Published each year		
1.2.3 Proportion of participants in front-line professional learning training sessions rating eSafety's educational and training as relevant or very relevant to their role.	≥ 90%	Maintain		

Rationale:
 Through research, education and training programs, we work to set a foundation to prevent online harm. We co-design and develop evidence-informed resources and advice to increase the online safety and resilience of groups most at risk of online harm.

Methodology:
1.2.1 Case study analysis of new resources published throughout the year.
1.2.2 Publication of threat assessment on the eSafety website.
1.2.3 Collection of ratings from participants in eSafety professional learning and front-line worker training sessions.

PBS links:
Program 1.3 – Office of the eSafety Commissioner
 Support positive online experiences through national leadership and administration of statutory schemes and educational and awareness activities that promote online safety for all Australians.

- Promote online safety for all Australians

Key activity 2

eSafety remediates online harms through our investigations and regulatory schemes, working with industry to build accountability and compliance in response to reported and identified harms.

Performance area 2.1: Reporting schemes

Intended result: eSafety's regulatory decision-making across our four reporting schemes is proportionate, consistent, fair and informed by evidence.				
Performance measure	Targets			
	2022-23	2023-24	2024-25	2025-26
2.1.1 Proportion of CB and ACA complaints or reports received, triaged and assigned to an investigator within 3-hour timeframe.	≥ 70%	Maintain from previous year		
2.1.2 Proportion of IBA complaints or reports responded to within two business days.	≥ 90%	Maintain from previous year		
2.1.3 Proportion of critical OCS investigations finalised within two business days. ¹	≥ 90%	Maintain from previous year		

Rationale:

The Online Safety Act gives us powers to protect all Australians across four reporting schemes: the Adult Cyber Abuse Scheme (ACA), the Cyberbullying Scheme for Australian children (CB), the Image-Based Abuse Scheme (IBA), and the Online Content Scheme for illegal and restricted content (OCS).

We give responsive and compassionate help to people experiencing a range of online harms. Once someone reports harmful content to us, we aim to alleviate or reduce the harm as quickly as possible.

Measuring the outcome or satisfaction level for individual complainants is difficult due to the need to protect their privacy and the sensitive nature of the harms people report. We will consider methods to quantitatively measure individual outcomes in future years.

Methodology:

- 2.1.1** Analysis of data which captures creation of reports and changes in report status.
- 2.1.2** Analysis of data which captures creation of reports and changes in report status.
- 2.1.3** Analysis of data which captures creation of reports and changes in report status.

PBS links:

- Program 1.3** – Office of the eSafety Commissioner
- Support positive online experiences through national leadership and administration of statutory schemes and educational and awareness activities that promote online safety for all Australians.
 - Operation of statutory schemes

¹Critical investigations include regulatory investigations into child sexual exploitation material, material advocating the doing of a terrorist act, and material inciting, promoting or instructing in matters of crime and violence.

Performance area 2.2: Effective regulatory actions

Intended result: eSafety takes effective action to remove material causing online harms.				
Performance measure	Targets			
	2022-23	2023-24	2024-25	2025-26
2.2.1 Proportion of total actionable IBA, ACA and CB complaints where material is removed	≥ 80%	Maintain		

Rationale:
We use our regulatory powers assertively but judiciously. We take both formal and informal actions to get results for people reporting online harms through the IBA, ACA and CB schemes.

Methodology:
2.2.1 Analysis of data which captures the total number of all actionable IBA, ACA, and CB complaints that result in material being removed.

PBS links:
Program 1.3 – Office of the eSafety Commissioner
Support positive online experiences through national leadership and administration of statutory schemes and educational and awareness activities that promote online safety for all Australians.

- Operation of statutory schemes

Key activity 3

eSafety promotes proactive and systemic change, working with online industries, users, educators, governments and their agencies to reduce the threat surface for online harms, lift overall standards of online safety across industry and deliver a more positive online experience.

Performance area 3.1: Industry codes/standards

Intended result: Industry codes are registered, or industry standards are determined.				
Performance measure	Targets			
	2022-23	2023-24	2024-25	2025-26
3.1.1 Proportion of industry sections with industry codes registered, or industry standards determined.	100% (All 8 sections have industry code/standards in place)	Maintain commitment and extend to include second round of industry codes or industry standards in 2023-24; monitoring and enforcing Industry Code/Standard compliance		

Rationale:

The Online Safety Act, provides for industry bodies or associations to develop codes to regulate certain types of harmful online material, and for eSafety to register the codes. The development and registration of the first round of industry codes (or the determination of industry standards if proposed codes do not provide appropriate community safeguards) is expected in 2022-23. Industry participants will likely need to start complying with commitments contained in codes or standards from 2023-24, including the provision of annual reporting, although the timing for commencement will depend on the final version of the codes submitted by industry.

Methodology:

3.1.1 Registration of industry codes or determination of industry standards.

PBS links:

Program 1.3 – Office of the eSafety Commissioner

Support positive online experiences through national leadership and administration of statutory schemes and educational and awareness activities that promote online safety for all Australians.

- Industry codes

Performance area 3.2: Basic Online Safety Expectations

Intended result: The Basic Online Safety Expectations are operationalised.				
Performance measure	Targets			
	2022-23	2023-24	2024-25	2025-26
3.2.1 Publication of regulatory guidance for relevant industry on the Basic Online Safety Expectations.	Expectations are published	Maintain		
3.2.2 Issuing of non-periodic reporting notices.	Initial set of notices issued	Notices are issued in accordance with phased approach		

Rationale:

The Basic Online Safety Expectations (the Expectations) are a crucial element of the Online Safety Act. eSafety intends to take a phased approach to exercising powers related to the expectations starting with the use of non-periodic notices, with a focus on specific expectations and acute issues of particularly high harm, such as child sexual exploitation and abuse. eSafety will use the information gathered from notices to build an understanding of industry practices, alongside other sources of evidence and insight. Future performance measures may include:

- Using the Expectations' reporting powers to seek unique insights, and improve industry's transparency and accountability, and/or use enforcement powers where industry is non-responsive.
- Expanding reporting to other major online harms and tracking key metrics over time by using periodic reporting powers.
- Providing further regulatory guidance where needed on the steps that industry could take to implement the expectations.
- Measuring compliance with notices, particularly to precision questions.
- Begin using statements of compliance or non-compliance to incentivise industry to improve safety processes.

Methodology:

3.2.1 Publication of the regulatory guidance

3.2.2 Case study analysis of systemic harms, crucial safety vulnerabilities and transparency gaps.

PBS links:

Program 1.3 – Office of the eSafety Commissioner

Support positive online experiences through national leadership and administration of statutory schemes and educational and awareness activities that promote online safety for all Australians.

- Basic Online Safety Expectations















Regulatory performance

Through a renewed deregulation agenda, the Australian Government is focusing on lifting regulator performance, capability and culture. To achieve these expectations and comply with best practice, we have developed tailored performance monitoring and reporting processes.

Our strategic objectives and performance measures directly support the accomplishment of the Australian Government's three principles of regulator best practice:

- 1. Continuous improvement and building trust:** regulators adopt a whole-of-system perspective, continuously improving their performance, capability and culture, to build trust and confidence in Australia's regulatory settings.
- 2. Risk-based and data-driven:** regulators maintain essential safeguards, using data and digital technology to manage risks proportionately to minimise regulatory burden and support those they regulate to comply and grow.
- 3. Collaboration and engagement:** regulators are transparent and responsive, implementing regulations in a modern and collaborative way.



		Principles of regulator best practice		
Key activities	Performance area	Continuous improvement / building trust	Risk-based and data-driven	Collaboration and engagement
Prevention – Using a solid evidence base, eSafety designs and delivers educational materials to prevent online harms, working with key sectors and community members to build user capability and resilience through training programs, awareness raising and referrals.	1.1 Educating Australians			
	1.2 Understanding of needs			
Protection – eSafety remediates online harms through our investigations and regulatory schemes, working with industry to build accountability and compliance in response to reported and identified harms.	2.1 Reporting schemes			
	2.2 Effective regulatory action			
Promoting systemic change – eSafety promotes proactive and systemic change, working with online industries, users, educators, governments and their agencies to reduce the threat surface for online harms, lift overall standards of online safety across industry and deliver a more positive online experience.	3.1 Industry codes/ standards			
	3.2 Basic Online Safety Expectations			



esafety.gov.au