

# eSafety

## CORPORATE PLAN

2023-2024



## **Acknowledgement of Country**

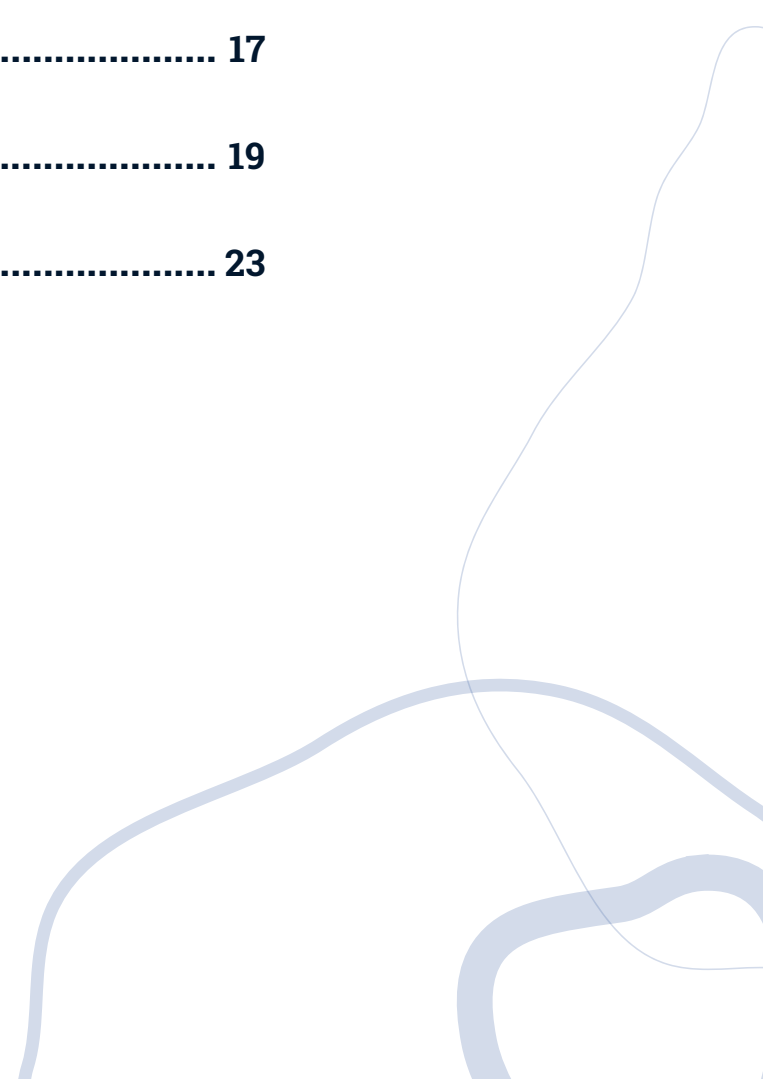
eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses – land, waters and community. We pay our respects to First Nations people, and to Elders past, present and future.





# Contents

<b>From the Commissioner .....</b>	<b>1</b>
<b>About us .....</b>	<b>3</b>
<b>Our purpose .....</b>	<b>4</b>
<b>Our key activities .....</b>	<b>5</b>
<b>Corporate planning framework .....</b>	<b>7</b>
<b>Our environment .....</b>	<b>9</b>
<b>Our capability .....</b>	<b>13</b>
<b>Risk management .....</b>	<b>17</b>
<b>Cooperation and partnerships.....</b>	<b>19</b>
<b>Our performance .....</b>	<b>23</b>





# Commissioner's foreword



## I am pleased to present the eSafety Commissioner's corporate plan for 2023-24.

This document outlines our vision, objectives, and priorities for the reporting periods 2023-24 to 2026-27. It brings together contributions from our team members, stakeholders and partners.

The corporate plan reflects our commitment to grow and to innovate, to stay true to our core values and principles, and to continue to meet our mandate of making sure Australians have safer and more positive experiences online.

The plan also gives the Australian Parliament, the public and all our stakeholders an understanding of our purpose and objectives. It details our functions and our roles, outlines what we will do to achieve our goal, and explains how we will measure our performance.

As a regulator, we operate in a rapidly changing and sometimes volatile environment. Often, the issues are complex. Our success depends on our ability to adapt to new challenges, seize opportunities, stay ahead of the technology curve, and stay in touch with the social dynamics of these post-COVID times.

Our corporate plan is designed to help us navigate these challenges.

We continue to see complaints increase across all our reporting schemes. So, it's imperative we continue to build our evidence base and our resources to reach more Australians with advice and support and enhance people's ability to report online abuse to us.

This is why at the heart of our corporate plan you will find a focus on people – every Australian who uses the internet to work, learn, play and connect. Our role as Australia's independent online safety regulator – the world's first – demands we deliver comprehensive, compassionate and people-focused services.

We will continue to help prevent online harms from occurring – through research, education programs and raising awareness.

We will continue to protect Australian citizens – through regulatory schemes and investigations under the *Online Safety Act 2021*.

And we will continue to drive proactive and systemic change – by forecasting technology trends, supporting industry to improve user safety standards, and strengthening our impact across borders.

In this plan, we also recognise the importance of protecting the environment, supporting our communities, and ensuring the well-being of our employees and stakeholders.

As a living, breathing roadmap, this plan will evolve and adapt as we progress. It will guide our decision-making, help determine resource allocation, and govern performance management. It also outlines the specific actions and initiatives we will take to achieve our objectives.

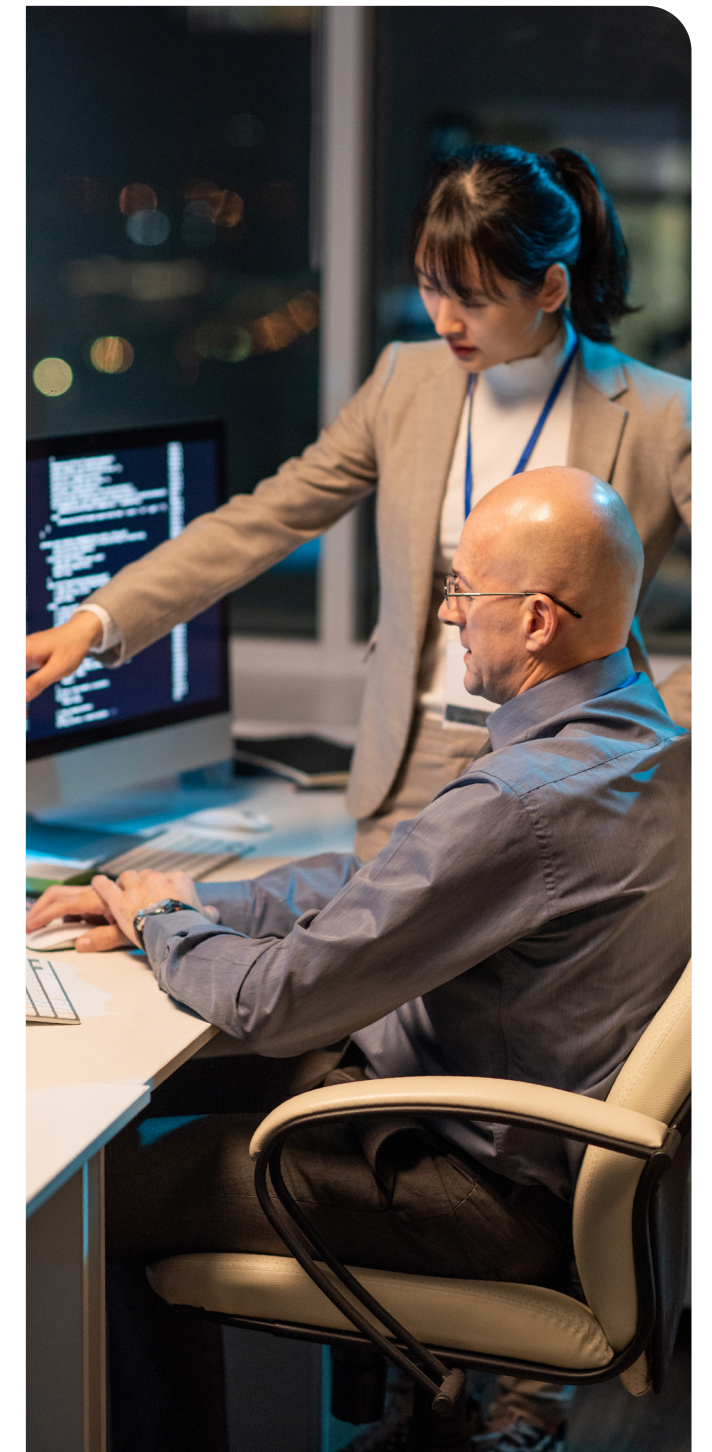
We have a clear set of expectations from the Australian Government. I am confident this plan will help us meet those expectations and allow us to continue to develop and succeed in the years to come, as we work towards becoming a modern, sophisticated and anticipatory regulator.

I would like to thank my eSafety colleagues and our stakeholders and partners for their input in developing this plan. I look forward to working together to turn its intention into reality and achieve our shared vision for the future.

Thank you for your support and for your commitment to online safety.

A handwritten signature in black ink that reads "Julie Inman Grant".

**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 legislation of its kind anywhere in the world, governs the functions of eSafety and includes a world-leading initiative – the Basic Online Safety Expectations – as well as the development of industry codes or standards to regulate illegal and restricted content. The 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 material during an online crisis event.

The eSafety Commissioner is an independent statutory office holder supported by staff from the Australian Communications and Media Authority (ACMA). In line with the Australian Government's Statement of Expectations and eSafety's Statement of Intent, the eSafety Commissioner has prepared this corporate plan consistent with the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and related legislation and guidance material. This corporate plan should be considered complementary to the ACMA's corporate plan.



## Purpose

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

## Vision

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

## Values

Our culture and values support us to achieve our purpose, now and into the future. We are committed to the Australian Public Service (APS) values of being impartial, committed to service, accountable, respectful and ethical.

Complementing the APS values, we have developed our own eSafety-specific 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

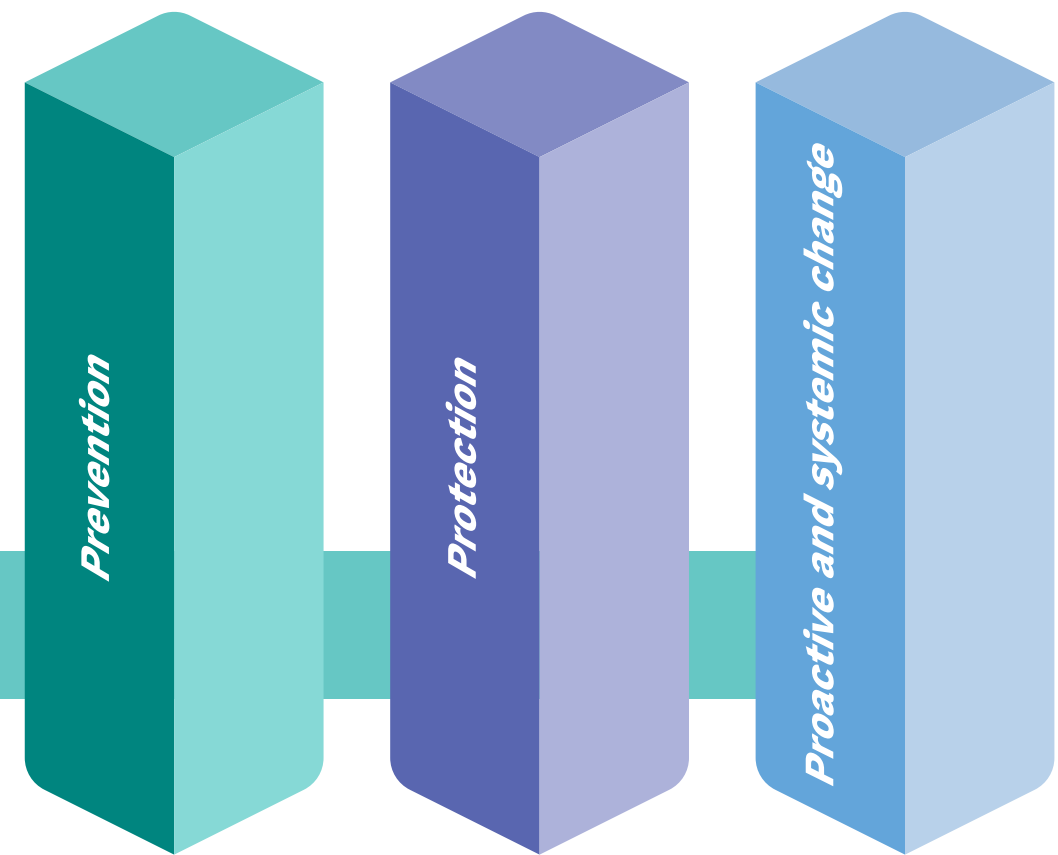


## We achieve our purpose through three key pillars

**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.



Further information on our strategic priorities can be found in the [Australian Government's Statement of Expectations](#) and our corresponding [Statement of Intent](#), and the [eSafety Strategy 2022-25](#).



# 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 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 to deliver more positive online experiences for Australians.

## Capabilities

Activities that enable us to deliver on our purpose.





# Our environment



**The past few years have seen an enormous shift to online learning, working, communicating, socialising and accessing services, and these trends – perpetuated through the COVID-19 pandemic – are exposing millions of Australians to increased risk of online harms.**

Advances in technologies, such as machine learning, artificial intelligence (AI) - including generative AI - and immersive technologies will continue to escalate online connections, communication, entertainment, sharing and learning 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, such as through the Digital Platform Regulators' Forum (DP-REG).

We are closely monitoring how our environment is evolving and shaping our operating context to 2027 and beyond, and we have developed this corporate plan within this context.

## Global environment

As the world's first government regulator 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.

While Australia remains an early mover and leader in online safety, internationally there are major legislative changes occurring. The European Union has enacted the Digital Services Act, and the United Kingdom Government is seeking to pass its Online Safety Bill. These new laws aim to regulate the systems and processes of online services more robustly and come with major penalties for non-compliance.

To prevent a fragmented international regulatory environment that will impede proactive change and regulatory impact, we continue to share our regulatory experience with like-minded governments and their regulatory agencies to promote global online safety regulation. This includes continuing our role and growing the membership of the Global Online Regulators Network, which was established in 2022. Current membership includes regulators in Fiji, Ireland and the United Kingdom.

## 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 emerging technologies to anticipate and remediate potential harm, while also harnessing opportunities for technology to promote safety. Our position papers on technology trends and challenges can be found at [Tech trends and challenges | eSafety Commissioner](#). Ongoing areas of focus 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 remove illegal and seriously harmful content at scale. However, as outlined in our [position paper](#) on algorithms and recommender systems, these tools also have the potential to contribute to online harms by amplifying content. There is also often limited transparency and accountability regarding the design, impact and operation of these tools.

Rapidly evolving generative AI technologies bring a more complex and urgent imperative to find ways to build technological skills and capabilities to be able to keep pace with the threat environment. Potential harms include new forms of Child Sexual Abuse Material (CSAM), image-based abuse, and children's exposure to synthetic sexually explicit content, conduct or contact. With growing data sets and parameters, recent generative AI has displayed emergent abilities that were previously unknown. This adds an element of unpredictability to future harms, though we anticipate existing detection, reporting and user authentication interventions will continue to be important.

### 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. Since publishing our [position paper](#), eSafety has contributed to ongoing policy discussions and continued to explore how this issue may present itself with new technologies.

### 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 typically limited in their ability 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. With an increasing number of services offering end-to-end encryption, eSafety is continuing to revise its [position paper](#) to accurately capture the current environment.

### Age assurance

Children and young people are at higher risk of being exposed to a range of online safety issues. The responsibility 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 for them.



In March 2023, eSafety submitted to the Australian Government an ‘age verification roadmap’ containing recommendations in relation to age verification and complementary measures to prevent and reduce harm associated with children and young people’s access to online pornography. While the government considers the roadmap and its recommendations, eSafety will draw on relevant insights to inform our approach to age assurance in related workstreams, such as the Basic Online Safety Expectations, the second phase of industry codes, and the development of educational resources.

### **Immersive environments and Web3.0**

Emerging technologies and evolving online environments present exciting opportunities for innovation, accessibility and new experiences. However, with speculation that the new version of the internet (Web3.0) may involve hyper-realistic immersive technologies and increasingly decentralised systems, there are also increasing concerns for online safety, privacy, and security, with potentially limited safeguards and accountability. Advances in tech wearables, high-sensory experiences, and synthetic media such as deepfakes (used to falsely depict a person), often created with generative AI, provide new vectors for abuse, violence, and ways to exacerbate harms for users and society. Whilst the extent that these technologies will be adopted, and at what pace and form, is still unknown, it is important safety guardrails and good governance are considered at the forefront and built into new developments at the earliest stages.

eSafety is working with industry, governments, and global experts to anticipate and prevent these harms and enhance transparency measures.

### **Fiscal environment**

The 2023-24 Portfolio Budget Statements provide eSafety with funding of \$51.181m and an average staffing level cap of 164 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 directs the ongoing work of eSafety, including eSafety’s role in the development of industry codes and/or industry standards throughout 2023 and the exercise of eSafety’s powers in connection with the Basic Online Safety Expectations.

The Australian Government has published its response to the House Select Committee’s Inquiry into Social Media and Online Safety. The Australian Government is pursuing three immediate priorities: the effective implementation and ongoing review of the Online Safety Act, tackling gaps in the current framework and supporting cross-government coordination on the regulation of online harms.

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 review of the Privacy Act, including proposals for the development of a Children’s Online Privacy Code
- the Australian Government’s response to the recommendations for regulatory reform in the Australian Competition and Consumer Commission’s (ACCC) fifth report of the Digital Platform Services Inquiry
- new information-gathering, code registration and standard-making powers for the ACMA in relation to disinformation and misinformation
- proposed reform to the National Classification Framework
- any reforms arising out of the Senate inquiry into international digital platforms and the Select Committee on Foreign Interference through Social Media.

## **Our response in this evolving environment**

We have designed a fit-for-purpose operating model which is intended to help us foster our regulatory maturity and operate as efficiently and effectively as possible. The operating model will support eSafety to deliver on our purpose and key activities.

### **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 administering four complaints and investigations schemes: the Adult Cyber Abuse Scheme, the Cyberbullying Scheme, the Image-Based Abuse Scheme and the Online Content Scheme. These schemes compel the removal of abusive and harmful content, limiting the ability of perpetrators to continue their abuse, and enable eSafety to take enforcement action against those platforms and service providers who fail to comply with regulatory notices. Further information can be found at [Regulatory schemes | eSafety Commissioner](#).

### **Proactive and systemic change**

Using data from our complaints and investigations schemes, along with research, consultation with industry and subject matter experts, and horizon scanning, eSafety works to achieve proactive and systemic change from the online industry.

Our Safety by Design initiative includes voluntary guidance material and tools that industry can use to conduct risk assessments of their products and services, and lift safety standards to better protect their customers’ safety and rights.

We also have powers to require mandatory reporting from service providers on how they are meeting the Basic Online Safety Expectations and keeping Australians safe online. The obligation to respond to a reporting requirement is enforceable and backed by civil penalties. eSafety publishes statements about the extent to which services are meeting the Basic Online Safety Expectations. These powers are intended to promote greater transparency from service providers and hold them accountable for their users’ safety. Further information can be found at [Basic Online Safety Expectations | eSafety Commissioner](#).

The Online Safety Act provides for industry bodies or associations to develop codes to regulate certain types of harmful online material. The first phase of industry codes or industry standards focus on reducing the risk of illegal content, such as child sexual abuse material, on online services. Further information on the development of the codes can be found at [Industry codes | eSafety Commissioner](#). If an industry code is found not to provide appropriate community safeguards, the eSafety Commissioner will not register the code and is able to determine an industry standard for the relevant section of the online industry.

# Our capability



## 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 new government initiatives. Subsequently, there has been a commensurate increase in the size of our workforce. The 2023-24 Federal Budget provided ongoing and stable base funding for eSafety, which provides organisational certainty and a reduced reliance on temporary staffing arrangements. 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 the reporting period, we will continue to embed these processes to ensure our operations are aligned with the wider APS Reform agenda and to deliver the best results for the Australian people.

The rate of technological change is rapid, and 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. Over this period, we will significantly reduce our reliance on external talent and invest further resources to develop and enhance our own staff's capability and productivity. We will develop an organisational capability strategy that will seek to address this challenge.

### Workforce planning

There is both opportunity and a 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 reporting period, we will invest in our reporting and analytical frameworks to make sure we have the right information and analysis 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 continue to 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 APS offerings within the ACMA training program and the APS Academy. Given our unique profile and the technological complexity of our regulatory sphere, eSafety will also need to harness expertise from the technology, academic and non-governmental organisation (NGO) communities.

## Wellbeing

We prioritise employee health and wellbeing, providing information, advice, and safe and healthy work environments for our employees. A firm commitment to staff wellbeing has allowed us to exceed our strategic objectives in this difficult operating environment. For the duration of this reporting period, 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 key 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 and other frontline work.



## Technology and digital capability

Our technology and digital capability underpins all the work of eSafety and is a key enabler in helping us achieve our purpose and objectives. Our technology strategy and roadmap outline the work underway to equip eSafety with the ICT, digital and data systems we need to deliver on our regulatory functions and strategic priorities. 2023-24 will see the development of a new three-year ICT Strategy and Roadmap to align with eSafety's future funding position, the eSafety Strategy 2022-25 and the eSafety Corporate Plan 2023-24 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 investigations technologies and technical capabilities**

We will continue to develop and maintain the technologies that enable eSafety to carry out its regulatory remit, while ensuring investigator wellbeing and operational efficiency through optimised systems. This work will include implementing new 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 and/or industry standards. It also includes enhancing in-house technical capabilities to continue to grow eSafety's regulatory maturity and expertise into the future in the face of complex emerging technologies.

### **Enable eSafety as a data-driven organisation**

We will continue to implement our Data and Information Management Roadmap, enhancing eSafety's governance and analytics capabilities to support data-driven decision making, regulatory prioritisation and transparency. This also includes finalising implementation of 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, governance and cyber security capabilities**

We will continue to modernise our IT 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 cyber security governance, in collaboration with the ACMA, and optimise technology investments 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, 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 PGPA Act, and the Commonwealth Risk Management Policy, including oversight from the ACMA Audit and Risk Committee and the eSafety Risk and Compliance Committee. In addition, eSafety has developed an eSafety Risk Guide and eSafety-specific templates to support risk management activities. 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 Advisory Committee (RAC) supports the eSafety Commissioner in providing advice about the exercise of key statutory powers, significant regulatory decisions 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. It safeguards consistency and objectivity and ensures key regulatory decisions have broad considered input from relevant areas of eSafety.

## 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 those most at risk of online harms including women, First Nations people, people with disability, LGBTIQ+ and CALD communities — 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 — A flexible, capable workforce operating under a regulatory model which allows for high levels of team support and/or provision of surge capacity — 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	Regular meetings between eSafety and the Minister for Communications — Leadership, coordination and 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
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
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 — Increased focus on outreach and awareness raising activities
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 and partnerships



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 regulator, 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.

We work closely with law enforcement partners across Australia and formalise these arrangements via Memorandums of Understanding (MOUs). As the threat environment evolves, we are committed to ensuring that these MOUs are up to date and fit for purpose.

Given the significant work underway internationally to regulate the digital environment, eSafety continues to engage with global counterparts to help shape discussions and decisions on the future of online safety and digital platform regulation. These engagements also provide an opportunity to learn from other countries approaches.

## ACMA

The Online Safety Act establishes the eSafety Commissioner as an independent statutory office holder, supported by the ACMA.

The ACMA provides corporate support services and staff to fulfil the functions of eSafety under section 184 of the Online Safety Act. As eSafety staff, except for the Commissioner, are staff of the ACMA, they are covered by ACMA entitlements, protections and obligations.

The effective provision of these support services is critical to our ability to fulfill our purpose and deliver results.



## Collaboration and cooperation – case studies

### Partnering for online safety education

eSafety works closely with school education bodies around Australia to support quality online safety education, share insights into issues impacting schools, raise awareness of reporting pathways, and provide professional learning opportunities for educators, webinars for parents and carers, and virtual classrooms for primary students. In 2022, eSafety established a National Online Safety Education Council to build on this work and foster greater cooperation with education sectors in each state and territory.

eSafety has also partnered with the Department of Education to provide professional learning to over 4,000 school chaplains on preventing and responding to cyberbullying. This work will continue under the new National Student Wellbeing Program, with professional learning provided to up to 10,000 Student Wellbeing Officers, supporting over 3,000 school communities each year until 2028.

### Partnering for prevention of technology-facilitated abuse in First Nations communities

eSafety collaborates with First Nations communities to build knowledge and awareness of technology-facilitated abuse and its emotional and psychological impacts. Through our online violence prevention strategy, eSafety is building the capacity of communities to tackle online abuse with culturally sensitive resources and education. We have established a collaborative partnership with the National Indigenous Australians Agency, and we continue to support the promotion of resources developed by Aboriginal Community Controlled Organisations under eSafety's Dedicated Project Officer Grants Program. In October 2022, eSafety launched its online learning module for First Nations community services. This professional development program has been co-designed with First Nations experts to assist frontline workers who support women experiencing technology-facilitated abuse as an extension of domestic and family violence.

### eSafety Youth Council

The eSafety Youth Council was appointed in April 2022 to give young Australians a direct line to the Australian Government and to ensure young people remain central in the decision-making process for policies and programs impacting them. The 24 council members, aged 13 to 24 years, are from a diverse range of experiences, genders, cultural and linguistic backgrounds, and locations.

In late 2022, the Council provided its views on different types of age verification and age assurance methods. This consultation informed the assessment of the age verification market and the suitability of tech options in eSafety's *Roadmap for Age Verification Report to Government on Mitigating Harms to Children and Young People from online pornography*. Most recently and notably, members wrote and produced an [open video letter to Big Tech and Social Media](#) heads urging they impose consequences on users who abuse and harass others, breaching platforms' terms of service. Media traction of the letter was strong, and as a result, leaders of tech companies including Amazon, Google, Meta, Microsoft, Pinterest, Snap, TikTok and Twitter met with the Council to continue the dialogue via a facilitated technology leadership session.



## Collaboration and cooperation – case studies

### Safer Internet Day

Safer Internet Day is a global online safety awareness-raising event celebrated in more than 170 countries. In Australia, eSafety is responsible for running the event, which is our biggest campaign each year.

In February 2023, we celebrated the 20th anniversary of Safer Internet Day, which prompted us to reflect on the importance of online safety awareness. Our **Connect. Reflect. Protect.** campaign encouraged Australians to use social media positively, consider the impact of their actions, and protect themselves and others by seeking advice from eSafety.

Our integrated marketing communications strategy, including outreach to stakeholders, strategic partnerships, media engagement, social media, paid media, email and webinars, helped us reach an estimated 11 million Australians. eSafety also had a record number of primary school students and teachers joining our virtual classrooms with 36,372 participants on Safer Internet Day and over 82,000 participants across the entire period of the campaign.

The campaign's success reflects the collaboration, hard work and creativity from eSafety and a broad range of stakeholders including educators, some of Australia's biggest corporations, individual Australians as well as the Prime Minister and a range of parliamentarians.

### Digital Platform Regulators Forum (DP-REG)

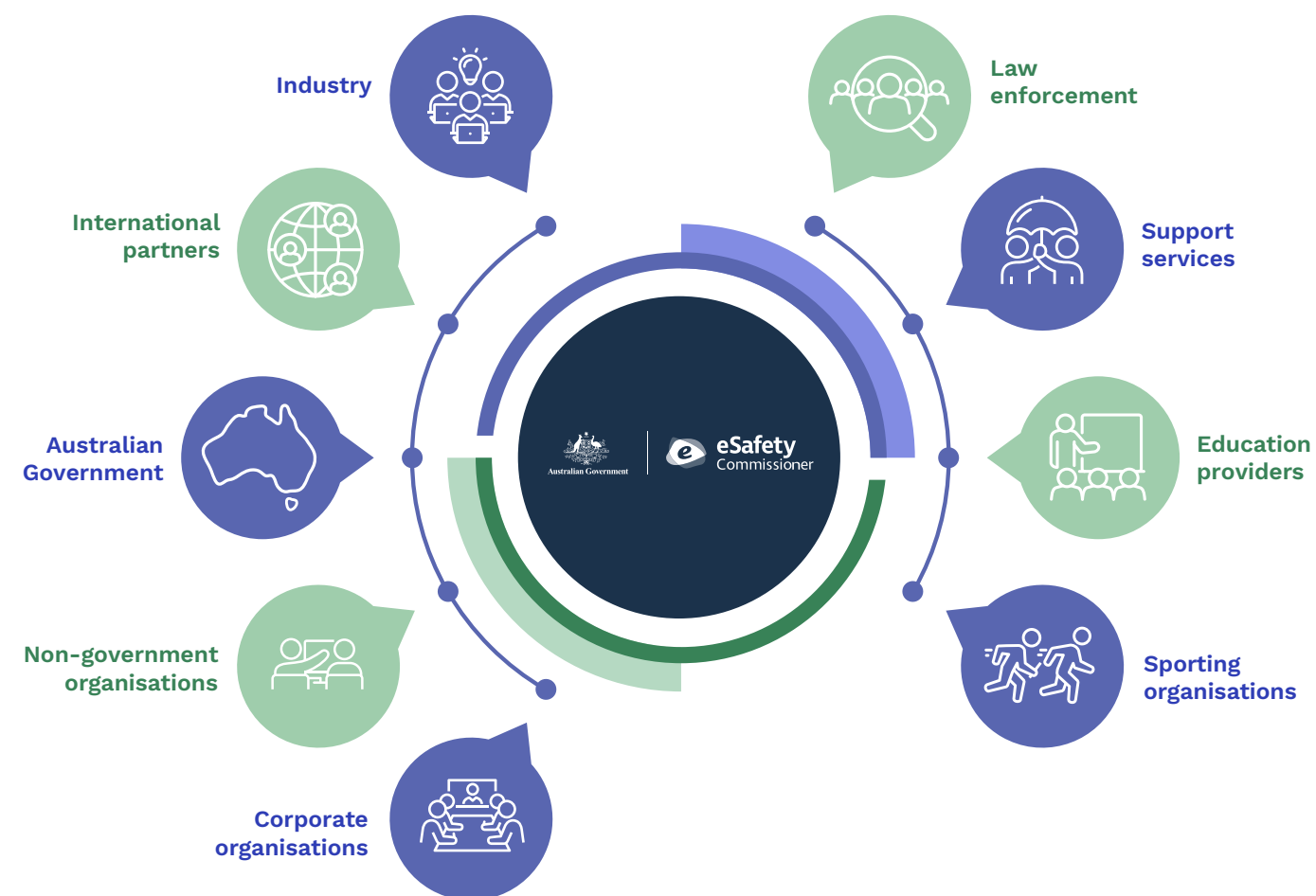
eSafety is a member of the [Digital Platform Regulators Forum](#) (DP-REG), an initiative of Australian independent regulators to share information about, and collaborate on, cross-cutting issues and activities on the regulation of digital platforms. Other members include the Australian Competition and Consumer Commission (ACCC), the Office of the Australian Information Commissioner (OAIC), and the ACMA.

DP-REG provides eSafety with an avenue to contribute its expertise to mutual areas of interest between members and obtain the benefit of other members' experience and expertise. Over 2022-23, the [priorities](#) for DP-REG included the impact of algorithms, enhancing transparency of digital platform activities and how they are protecting users from harms, and collaboration and capacity building between members.

### Global Online Safety Regulators Network

eSafety led the establishment of the [Global Online Safety Regulators Network](#), which was launched in November 2022, alongside regulators from Fiji, Ireland and the United Kingdom. The network brings together online safety regulators from around the world to share best practice and insights, and support coordinated approaches to online safety issues. Through this, we will encourage wider international membership and cooperation, with the aim of making sure the approach to online safety between countries is as consistent and coherent as possible. eSafety is the Chair of the network for 2023 and will oversee its expansion to new members and the operationalisation of the strategic plan and roadmap for action.

## Our stakeholders and partners





# Our performance



## 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

<b>Intended result:</b> Australians are enabled by education, training and resources to prevent online harms.				
Performance measure	Targets			
	2023-24	2024-25	2025-26	2026-27
1.1.1 Number of participants in frontline and professional learning training sessions.	10,100	Increase from previous year		
1.1.2 Number of unique visitors to eSafety websites.	1.5m	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 mitigate risk and 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** – 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.

- Australians are enabled by education, training and resources to prevent online harms.

Due to the nature of our work, the diversity of jurisdictions and stakeholders, the accessibility of data and the pace of technological change, it is difficult to measure effectiveness in some areas of our work. eSafety is working to mature our evaluation capabilities to support improved assessment of effectiveness for these areas in future years.

### Performance area 1.2: Understanding of needs

<b>Intended result:</b> 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			
	2023-24	2024-25	2025-26	2026-27
1.2.1 Proportion of educational 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 research reports and papers that build the evidence base relating to online safety for Australians.	6 reports or papers published	Maintain		
1.2.3 Proportion of participants in front-line professional learning training sessions rating eSafety's educational material 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, such as Aboriginal and Torres Strait Islander peoples, women, LGBTIQ+ communities, culturally and linguistically diverse communities, older Australians, people living with disability, young people, and children.

**Methodology:**  
1.2.1 Case study analysis of new resources published throughout the year.  
1.2.2 Number of published research reports on the eSafety website, or in peer-reviewed journals.  
1.2.3 Collection of ratings from participants in eSafety professional learning and front-line worker training sessions.

**PBS links:**  
**Program 1.3** – 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.

- Educational programs, strategies and tools are based on an understanding of the specific needs of groups most at risk of online harm.

## 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			
	2023-24	2024-25	2025-26	2026-27
2.1.1 Proportion of cyberbullying and adult cyber abuse complaints or reports received, triaged and assigned to an investigator within three-hour timeframe.	≥ 70%	Maintain from previous year		
2.1.2 Proportion of image-based abuse complaints or reports responded to within two business days.	≥ 90%	Maintain from previous year		
2.1.3 Proportion of critical Online Content Scheme investigations finalised within two business days. <sup>1</sup>	≥ 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** – 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.

- eSafety's regulatory decision-making across the four reported schemes is proportionate, consistent, fair and informed by evidence.

<sup>1</sup>Critical 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			
	2023-24	2024-25	2025-26	2026-27
2.2.1 Proportion of total image-based abuse, adult cyber abuse and cyberbullying 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 image-based abuse, adult cyber abuse and cyberbullying schemes.

The OC scheme is not included within this performance measure as we refer all CSAM to the INHOPE network to be removed. CSAM represents over 99% of all material reported to the OC scheme.

#### Methodology:

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

#### PBS links:

**Program 1.3** – 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.

- eSafety takes effective action to remove material causing online harms.



## 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 to deliver a more positive online experience.

### Performance area 3.1: Industry codes/standards

<b>Intended result:</b> Industry codes are registered, or industry standards are determined.				
Performance measure	Targets			
	2023-24	2024-25	2025-26	2026-27
<b>3.1.1</b> Proportion of industry sections with industry codes registered, or industry standards determined, for Class 1 material.	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 2024-25, as well as monitoring and enforcing compliance with applicable industry codes/standards.		

**Rationale:**  
The Online Safety Act provides for industry bodies or associations to develop codes for eight sections of the online industry to regulate certain types of harmful online material, and for eSafety to register the codes. If eSafety does not register an industry code that has been submitted, eSafety is able to determine an industry standard. The first phase of industry codes and industry standards are expected to be in place for all eight sections of the industry in 2023-24.

The eSafety Commissioner provided industry associations with her preliminary views on the first phase of draft industry codes in February 2023, inviting industry associations to respond and/or resubmit draft industry codes. eSafety received eight revised draft industry codes on 31 March 2023. On 31 May 2023, the eSafety Commissioner decided to register five industry codes and reserved her decision on one industry code. eSafety also announced it will develop mandatory industry standards for two sections of the online industry because the codes submitted for those sections failed to meet the legislative requirements. Code commitments will come into effect six months from registration. eSafety plans to commence work in connection with phase two of the industry codes development process (dealing with restricted content) in 2023-24.

**Methodology:**  
**3.1.1** Registration of industry codes or determination of industry standards.

**PBS links:**  
**Program 1.3** – 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 are registered or industry standards are determined.

### Performance area 3.2: Basic Online Safety Expectations

<b>Intended result:</b> The Basic Online Safety Expectations increase the transparency and accountability of online service providers and incentivise improvements in online safety.				
Performance measure	Targets			
	2023-24	2024-25	2025-26	2026-27
<b>3.2.1</b> Issuing of non-periodic reporting notices.	Issue 10 non-periodic notices	Maintain		
<b>3.2.2</b> Issuing of periodic reporting notices.	1 set of 5 periodic notices across a 24-month period	NA	1 set of 5 periodic notices across a 24-month period	NA

**Rationale:**  
The Basic Online Safety Expectations are a crucial element of the Online Safety Act. The Basic Online Safety Expectations Determination 2022 sets out the Australian Government's expectations that social media, messaging, gaming, dating, file-sharing services and other apps and websites will take reasonable steps to keep Australians safe. The current determination was registered on 23 January 2022.

Under the Online Safety Act, eSafety can require online service providers to report on how they are meeting any or all of the Expectations. eSafety has taken 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, publishing appropriate information in order to improve transparency and accountability. eSafety will continue to expand its use of powers under the Online Safety Act, including through further non-periodic notices focussed on specific harms, and periodic notices to track issues and improvements over time. Future performance measures may include:

- Collating case studies of changes made by industry following the identification of issues through notices.
- Measuring the use of information published by eSafety to hold industry accountable, including through academia, civil society, and the media.
- Beginning to use statements of compliance or non-compliance to incentivise industry to improve safety processes.

**Methodology:**  
**3.2.1** Issuing of non-periodic reporting notices.  
**3.2.2** Issuing of periodic reporting notices.

**PBS links:**  
**Program 1.3** – 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

The Australian Government is focused 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 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 manage risks proportionately and maintain essential safeguards while minimising regulatory burden, and leveraging data and digital technology to support those they regulate to comply and grow.
3. Collaboration and engagement: Regulators are transparent and responsive communicators, implementing regulations in a modern and collaborative way.



Key activities	Performance area	Principles of regulator best practice		
		Continuous improvement / building trust	Risk-based and data-driven	Collaboration and engagement
<b>Prevention</b> – Using a solid evidence base, eSafety designs and delivers educational materials to prevent online harms, working with education, NGOs, frontline workers, the community sector, industry and others to build user capability and resilience through training programs, awareness raising and referrals	1.1 Educating Australians	✓	✓	✓
	1.2 Understanding of needs	✓		✓
<b>Protection</b> – 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		✓	✓
<b>Promoting systemic change</b> – 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 to deliver a more positive online experience.	3.1 Industry codes/ standards	✓		✓
	3.2 Basic Online Safety Expectations	✓	✓	✓





[eSafety.gov.au](https://www.esafety.gov.au)