Industry Briefing: Online Safety Codes

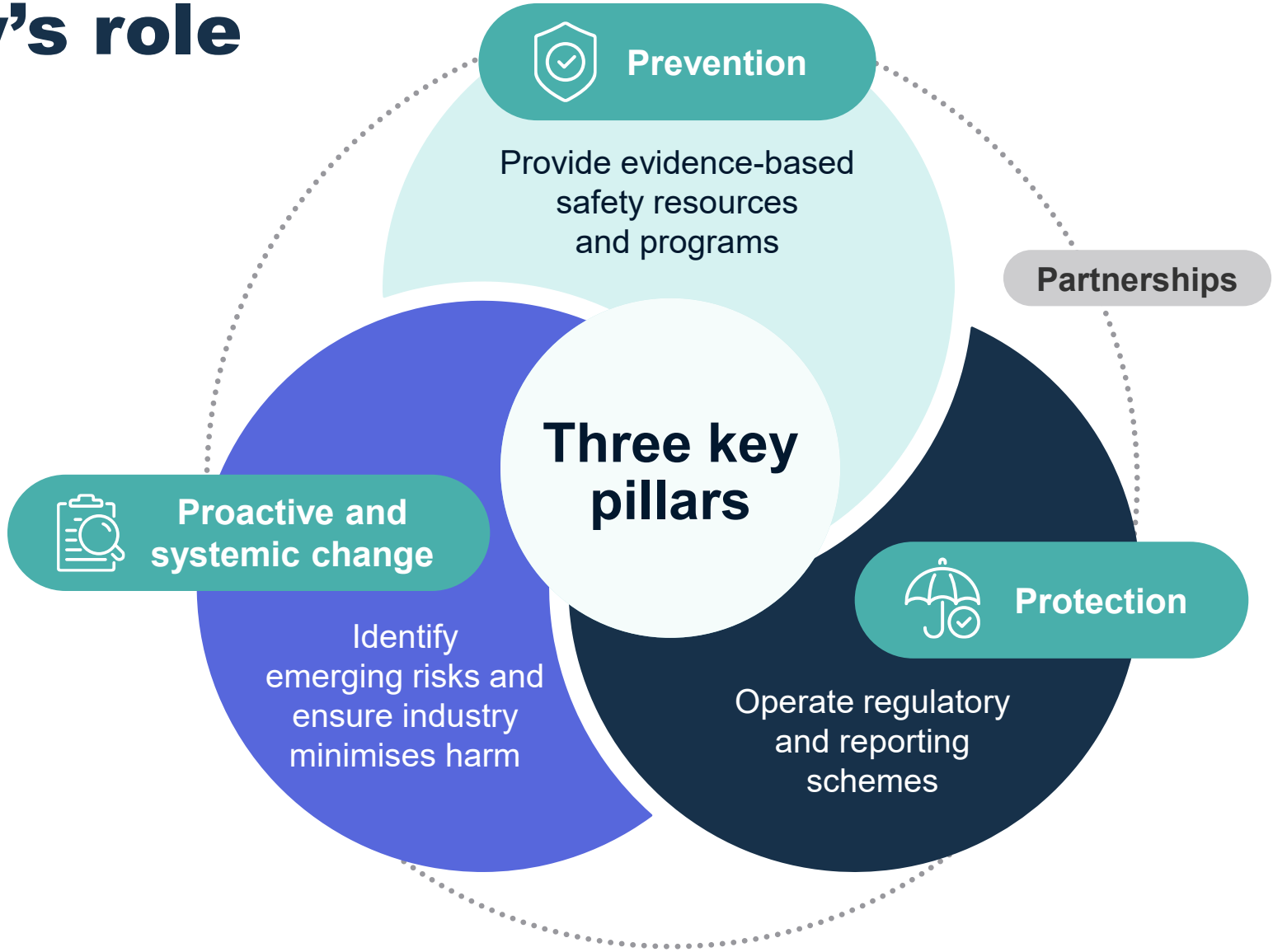
Ashley Katz, Manager – Industry Supervision

Chloe Bennett, Manager – Online Safety Codes

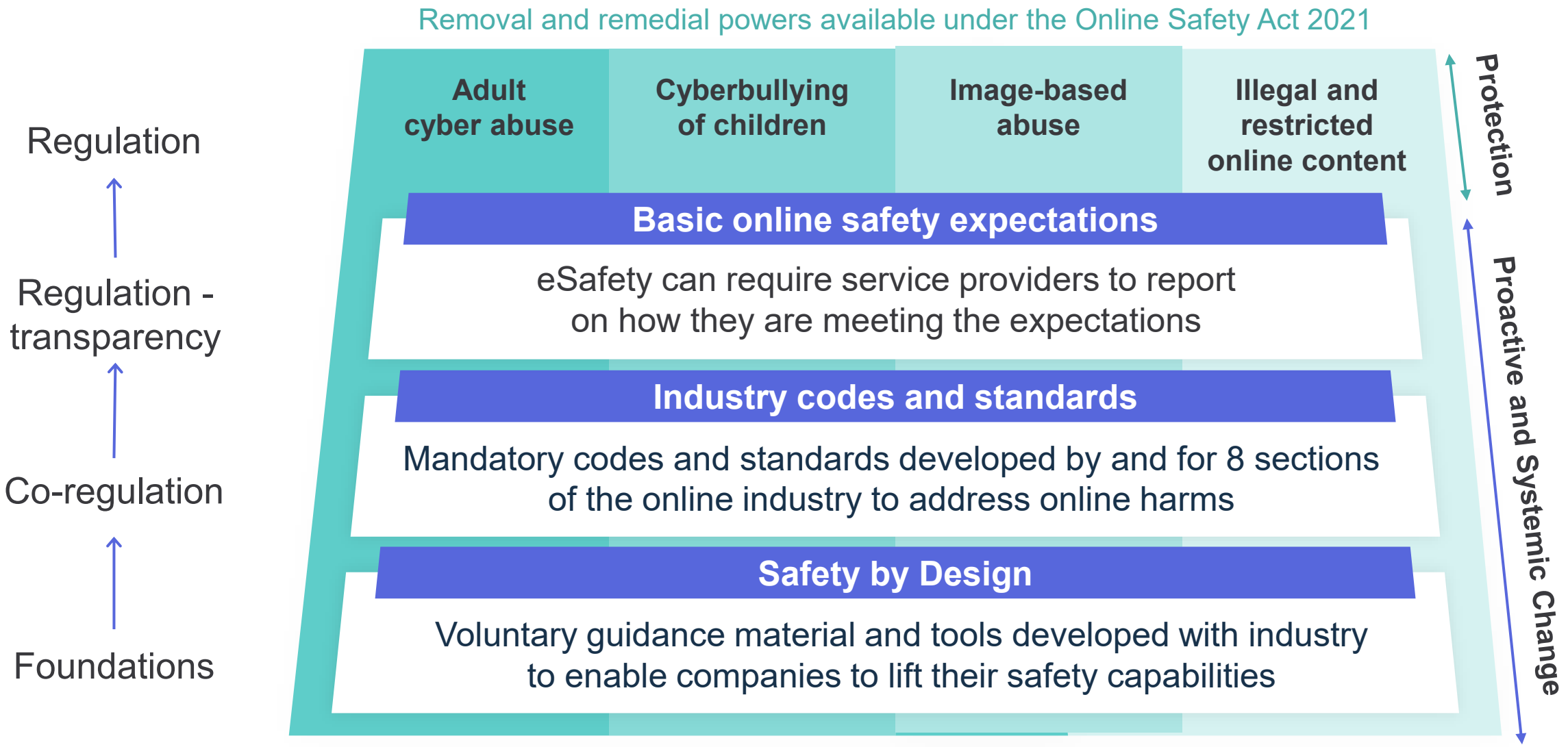
Australian Government

eSafetyCommissioner

eSafety's role



eSafety's regulatory framework



Online Safety Codes and Standards

Unlawful Material Codes & Standards

Class 1A & Class 1B (RC)

- Child sexual exploitation material
- Pro-terror
- Extreme crime and violence
- Crime and violence
- Drug related content

Age-Restricted Material Codes

Class 1C and Class 2 (X18+, R18+)

- Online pornography
- High-impact violence
- Material which instructs in/promotes self-harm, suicide, disordered eating
- Simulated gambling (*not including in-game purchases linked to elements of chance*)

8 sections of online industry

1. Social media services (SMS)
2. Relevant electronic services (RES) (e.g. services with messaging, chat features, online games played with other users)
3. Designated internet services (certain websites, apps, online file storage, gen AI services – where not SMSs or RESs)
4. Equipment manufacturers and suppliers
5. Internet carriage services (ISPs)
6. Hosting services
7. App distribution services
8. Search engine services

Key differences – Codes, Standards and SMMA

	Codes	Standards	Social media minimum age
Key focus	Access to material as defined in the National classification scheme	Access to material as defined in the National classification scheme	Raising the minimum age to hold accounts on certain types of services
Development	Codes are drafted by industry	Standards drafted by eSafety, after industry has made an attempt	Law enacted by Parliament
Legislative instrument	Not legislative instruments	Legislative instrument	Legislative instrument
Enforcement	eSafety can enforce civil penalties after a direction to comply	eSafety can enforce breaches immediately	eSafety and OAIC can enforce civil penalties immediately
Age assurance	Age-Restricted Material Codes require 'appropriate age assurance'	n/a	Requires reasonable steps to prevent age-restricted users from having accounts' on 'age-restricted social media'
Relevant age	18 years for Age-Restricted Material Codes	n/a	16 years

Unlawful Material Codes & Standards requirements

Detection
of known child sexual abuse and pro-terror material

Disruption
and deterrence for new child sexual exploitation and pro-terror material

Generative AI
requirements

Investment & resourcing
Safety investment, staffing and resourcing requirements

User reporting
measures requiring timely investigation and actioning

Safety by design
requirements

Age-Restricted Material Codes requirements

Age assurance
applying to legally age-restricted material.

Safety tools, options and information
accessible to adult users as well as kids.

Wide range of services
Including gaming services and services relating to gaming.

Investment & resourcing
Safety investment, staffing and resourcing requirements

User reporting
measures requiring timely investigation and actioning

Safety by design
requirements

ARM Codes: Development Timeline

- **July – October 2024:**
  - eSafety published Notices and Position Paper for the production of Age-Restricted Material Codes
  - Industry produced first draft of Codes
- **October 2024**
  - Preliminary Draft Codes received for all sections of the online industry. eSafety provided feedback on key issues
  - The drafting groups conducted public consultation on the Draft Codes during October/November 2024
- **December 2024:** Industry requested and received an extension of time to return Codes
- **February-May 2025:** Codes received and feedback provided; eSafety gave preliminary views on Code registrability in April; sought additional commitments particularly about chatbots
- **27 June 2025**: 3x Codes Registered (Internet Carriage Services/Hosting Services/Search Engine Services)
- **4 July 2025:** Further versions of remainder Codes submitted for assessment
- **9 September 2025:** 6x remaining Codes registered
- **9 March 2026 onwards:** Relevant measures for gaming services come into effect

Age-Restricted Material Codes – Focus Codes for Today's Presentation

Relevant Electronic Services Code (RES)
- Gaming services with communications functionality or limited communications functionality

Designated Internet Services Code (DIS) - Gaming services without communications functionality

App Distribution Services Code (APP) – Stores which sell games online

Equipment Code (EQP) - Equipment services such as phones, computers and gaming consoles

Measures across multiple ARM Codes

1. Communication and reporting requirements
2. Resourcing Trust and Safety Functions
3. Providing Appropriate Options, Tools and Information to End-users
4. Age assurance measures

Communication and reporting to eSafety obligations for service providers

- These obligations include:
  - Some **risk assessment** requirements
  - Updates on **relevant changes** to the service
  - Updates on **material changes** to the service
  - The **referral of unresolved end-user complaints**
  - Compliance reporting

	Designated Internet Services		Relevant Electronic Services		App Distribution Services		Equipment	
	Phase 1	Phase 2	Phase 1	Phase 2	Phase 1	Phase 2	Phase 1	Phase 2
Conduct risk assessment	✓	✓	✓	✓	✗	✓	✓	✓
Provide risk profile information	✓	✓	✓	✓	✗	✓	✓	✓
Update eSafety on relevant changes	✓	✓	✓	✓	✓	✓	✓	✓
Assess risk before making material changes	✓	✓	✓	✓	✗	✓	✗	✓
Refer unresolved complaints to eSafety	✓	✓	✓	✓	✗	✓	✗	✓
Submit compliance reports	✓	✓	✓	✓	✓	✓	✓	✓

Reports and complaints from end-users

Several ARM Codes require services to allow end-users to make reports and complaints, and to action these complaints in a timely manner

Providers must enable access to **easily accessible complaints forms**

Providers have obligations to **respond to and to action** reports

Providers must **have and comply with internal policies and procedures** for dealing with complaints

Unresolved complaints must be referred to eSafety in a prompt manner

Trust and Safety Functions

Measures include:

- Sufficiently **resourcing trust and safety functions** including to ensure Code compliance
- Sufficiently **training personnel** to deal with user reports in respect of harmful material
- Regularly reviewing **internal policies** relating to trust and safety functions
- Appropriately responding to **user questions/complaints** about safety
- **Continuously improving** safety tools, features and settings over time

Providing Safety Tools, Options and Information for End-users

Information Accessibility

Across the Codes different types of service providers must make available information about safety tools and options

Safety Tools

Various obligations to provide safety tools including for all end-users to limit receipt of types of class 1C or class 2 material

Links to other services

Some requirements to provide links to third-party services that have subject-matter expertise

‘Appropriate’ Age assurance: Head Terms clause 5.1(c); Regulatory Guidance Appendix F

(v) examples of age assurance measures that will be considered appropriate for the purposes of this Code include:

(A) matching of photo identification;

(B) facial age estimation;

(C) credit card checks;

(D) digital identity wallets or systems;

(E) attestation by a parent of age or whether an Australian end-user is a child;

(F) use of artificial intelligence technology to estimate age based on relevant data inputs;

(G) other measures meeting the requirements of section 8 (Confirmation of age) of the Online Safety (Restricted Access Systems) Declaration 2022; and

(H) relying upon appropriate age assurance measures implemented in respect of the relevant end-user by: (1) another party (whether another industry participant, government agency, a third party vendor or another third party) and confirmed by an age signal or other mechanism provided to the service provider by that other party; or (2) the service provider in respect of another service as contemplated in clause 5.1(c)(vi),

although this list is not comprehensive and additional age assurance measures may also be considered appropriate;

- Compared to some international jurisdictions, there is no minimum accuracy level for age assurance methods – instead must be ‘technically accurate, robust, reliable and fair’
  - No requirements for a particular type of age assurance
  - Self-declaration and contractual terms limiting child use will *not* be sufficient forms of age assurance
- Service providers should implement age assurance systems that are secure and reasonably resistant to circumvention.
- Fairness: ideally numerous methods of AA should be made available
- Must always remain in compliance with *Privacy Act 1988* (Cth) and associated APPs and Codes

RES Code Specific Requirements

Australian Government

eSafetyCommissioner

Requirements under the RES Code

Different obligations under the RES Code will apply depending on whether and how users are able to communicate with each other on the service

A gaming service with communications functionality

Games which allow you to play online with other end-users which enable the sharing of user generated URLs, hyper-linked text, images or videos between users.

A gaming service with limited communications functionality

Games which allow you to play online with other end-users where communication is not allowed or limited to:

1. in-game images or footage;
2. user-generated designs (such as environments and artwork);
3. virtual objects or maps;
4. pre-selected messages;
5. non-hyper-linked text that is subject to automated filtering technology;
6. ephemeral voice interactions.

Requirement for *both* types of gaming services in the RES Code: Appropriate Age Assurance

You must implement appropriate age assurance measures if you provide access to a game that:

- Is, or would likely be, classified as R18+ under the Classification Act because it constitutes simulated gambling material, or
- Is otherwise classified as R18+ in accordance with the Classification Act

Services that have to implement these measures must also take appropriate steps to **test and monitor the effectiveness of these age assurance measures** over time

- No risk assessments required

Obligations for gaming services with communications functionality (Table 11 RES Code)

A gaming service with communications functionality enables the sharing of user generated URLs, hyper-linked text, images or videos between users.

Having and enforcing terms and conditions prohibiting illegal activity

- Providers must prohibit end-users from sharing material via the service in the course of engaging in:
  - Non-consensual sharing of intimate images
  - Grooming of children
  - Sexual extortion (or sextortion)

  Where provider is aware of a breach they must take action in a timely manner.

- Other requirements include reporting mechanisms; staff training; requirements to notify eSafety of unresolved complaints and changes to the service; on-request reporting; end-user information requirements and continuous improvement requirements

Obligations for gaming services with limited communications functionality (Table 12 RES Code)

Applies to games rated R18+ only *or* games that contain simulated gambling and would likely be rated R18+

- Limited specific requirements
- Main requirements include providing safety information to end-users; on-request reporting to eSafety on Code compliance; and ensuring that services provide a complaints tool about code compliance

DIS Code Specific Requirements

Australian Government

eSafetyCommissioner

Relevant provisions: “Classified DIS”

Services will generally be captured under the Designated Internet Service Code *only* if they do not fall into the definition of an online gaming service under the RES Code.

This could include single player games *with online functionality* but with *no communications functionality*.

In this context, Classified DIS means a DIS that:

- Has the sole or predominant purpose of providing general entertainment, news or educational content, being:
  - Computer games that have been classified as R18+ Restricted or lower; or
  - Computer games that are exempt from classification under the Classification Act; or
  - Computer games that have not been classified but, if classified, would likely be classified R18+ Restricted or lower.
- Classified DIS are not required to undertake a risk assessment under the Code

Requirements for Classified DIS

- **Age assurance and access control**
  - Providers must implement appropriate age assurance measures before providing access to simulated gambling material.
  - Providers must take appropriate steps to test and monitor the effectiveness of these measures over time.

- **Appropriate measures to limit the risk of child end-users accessing or being exposed to other class 2A, R18+ and/or self-harm material**
  - Providers must implement appropriate measures that limit the risk of Australian children accessing or being exposed to this material

  - Other requirements include reporting mechanisms; resourcing trust and safety functions; on-request reporting to eSafety; notifications of changes in functions; end-user information provision requirements

App Distribution Services Code Specific Requirements

Australian Government

eSafetyCommissioner

Requirements in the APP Code - Risk Assessments must consider:

Adult apps: Apps rated 18+

Risk assessments must take into account matters including:

- whether adult apps are permitted on the service;
- the devices on which the app distribution service is made available;
- the ages of end-users and likely end-users of the app distribution service in Australia;
- the likelihood that the service may be used by an Australian child to download or access adult apps;
- the likelihood that a significant number of Australian children will access the service
- where applicable, design features and controls deployed to mitigate relevant risks

Requirements in the APP Code

After conducting a risk assessment, app distribution services with a high risk that children will download or purchase adult apps must implement appropriate age assurance to prevent children to do so.

Adult apps: Apps rated 18+

- **Clear Age/Content Ratings:** Providers must display age and content ratings clearly before download. Age ratings must be **appropriate.**
- **Policies for Rating Review:** Providers must have processes to assess appropriateness of app ratings.
- **Safety Tools & Resources:** Providers must offer and continuously improve safety tools and provide online safety resources explaining measures under the code.

Equipment Services Code Specific Requirements

Australian Government

eSafetyCommissioner

EQP Code

Interactive (Tier 1) Devices

- User-interactive – there is a two-way flow of material between the device and the end-user
- Personal and portable – may be carried with the end-user
- Capable of operation without the use of any other Interactive (Tier 1) Device
- General internet browsing through a screen or display capable of displaying video or images is an intended significant function of the device

Secondary (Tier 2) Devices – equipment that is not an interactive (Tier 1) device

- User-interactive
- May be personal or communal (intended for use by more than one end-user)
- Is capable of operation with or without the use of an interactive (Tier 1) device
- General internet browsing is not an intended significant function of the device

Other Interactive Devices - Equipment other than an interactive (Tier 1) device

- Has general internet browsing functionality as an intended significant function of the device, and
- Has functionality that enables an end-user to use their device to share material with end-users of other devices; OR
- Permits an end-user to view or search for other end-users for the purpose of communicating with them.

Requirements in the EQP Code

OS Providers of Interactive (Tier 1) Devices

- Required to allow end-users to set up **child and restricted accounts:** these accounts must have appropriate default safety settings that reduce the risk of such accounts being used to view online pornography
- Sharing details of whether a user is on a child or restricted account across services also provided by the OS provider
- Must allow an adult account holder on the device to adjust safety measures to a more restrictive level for shared devices

Requirements in the EQP Code

Tier 2 and ‘Other’ Interactive Devices

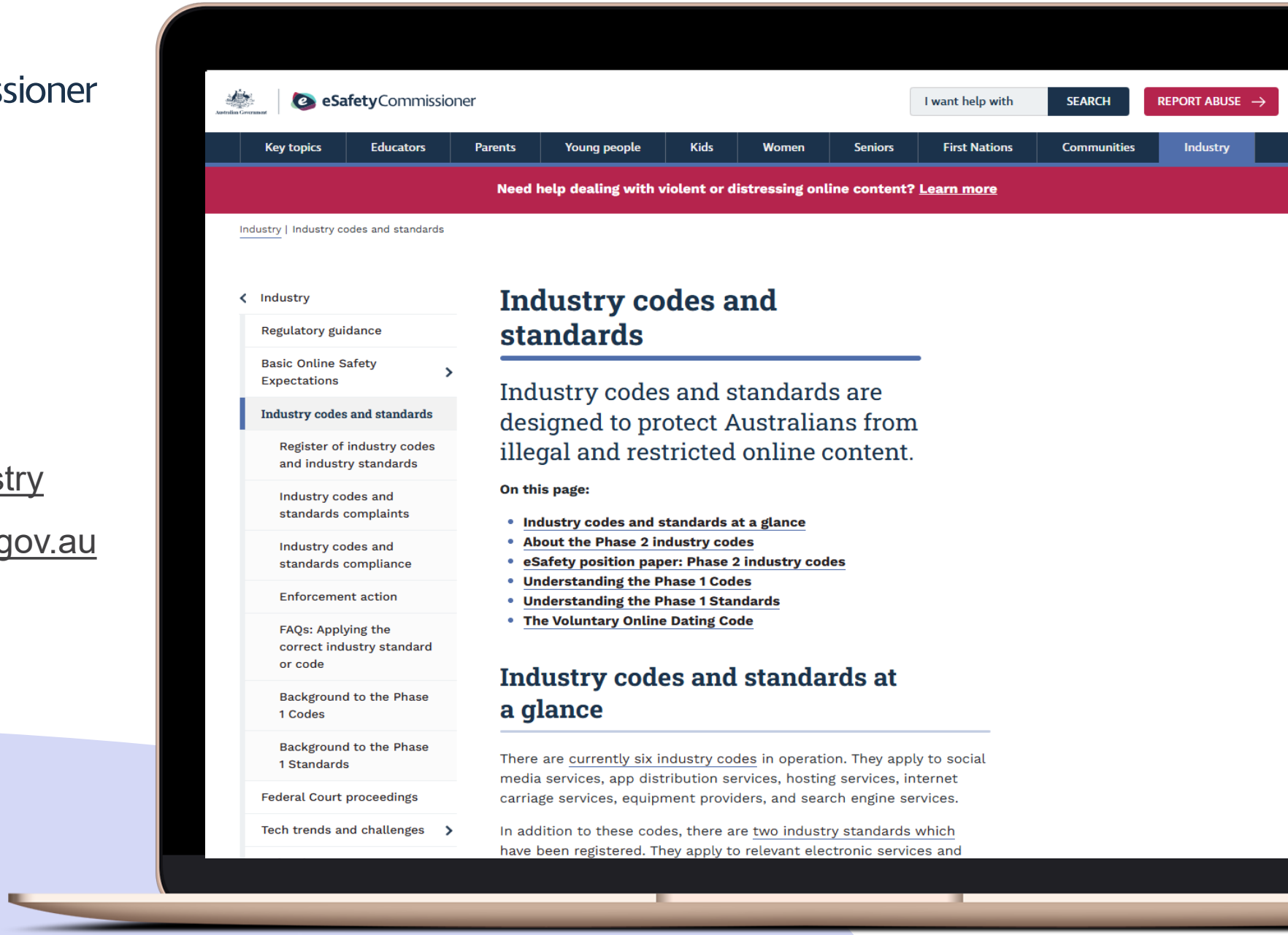
- Must provide tools, features and safety settings to assist end-users to manage children use experiences
- Provide end-users with safety information
- Must have sufficient personnel to oversee device safety (also applies to Tier 1)
- Updates to eSafety about relevant changes in technology
- On-request reporting to eSafety

Useful Resources

- Register of Industry Codes and Standards
- Regulatory Guidance on Online Safety Codes and Standards
- FAQs for End-Users and Regulated Entities
- Compliance Portal

Australian Government | eSafetyCommissioner

Thank you

https://www.esafety.gov.au/industry

Contact us at industry@esafety.gov.au