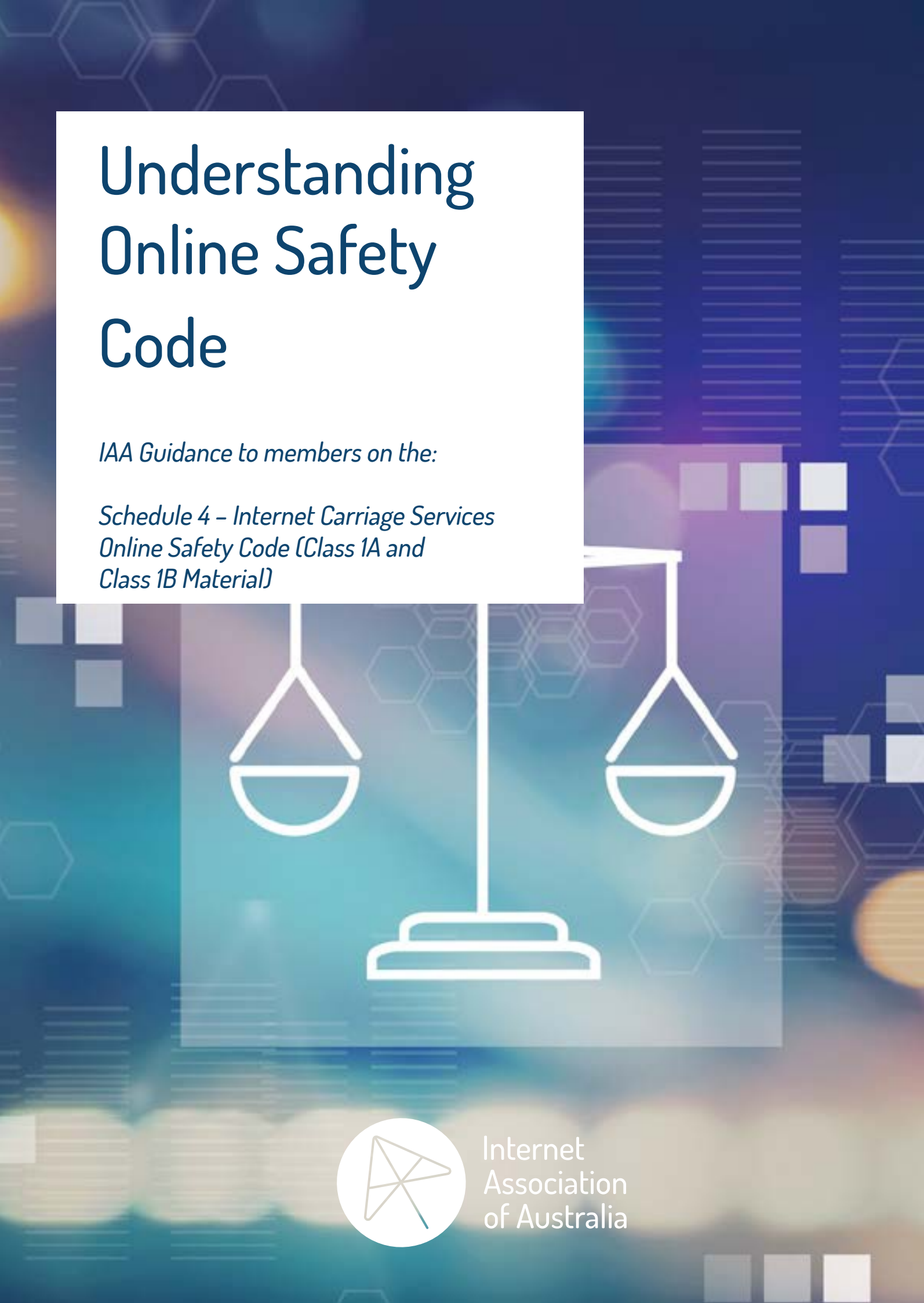
Understanding Online Safety Code

IAA Guidance to members on the:

Schedule 4 – Internet Carriage Services Online Safety Code (Class 1A and Class 1B Material)



Internet Association of Australia

Contents

Title: Understanding the Online Safety Code, IAA guidance to members
Author: Sophia Joo
Published: August 2023

Executive Summary

IAA's guide to the new Online Safety Code for Internet carriage services

On 16 June 2023, Schedule 4 - Internet Carriage Services Online Safety Code (Class 1A and Class 1B Material) ("**Code**") was formally registered by the eSafety Commissioner, under the *Online Safety Act 2021* (Cth) along with 4 other codes for other sections within the internet ecosystem.

These codes are intended to improve the safety of the online environment, specifically with regard to content involving sexual abuse of children, acts of terrorism, and extreme crime and violence material, as well as regulation over material inappropriate for children.

Recognising the limited role that internet service providers play in controlling the content accessible on the internet, the Code sets out limited minimum compliance requirements that apply to internet service providers.

This guide is designed to assist our members to understand and implement the compliance requirements of the Code. If your business operates other online services, other codes and compliance measures may apply.

NB: This guide does not, and does not intend to provide legal advice, and should not be taken as such.

Glossary

Appropriate: where used to qualify measures required under this Code, means measures implemented must be demonstrably reasonable, taking into account:

i. the importance of the applicable online safety objectives and outcomes specified in the Code Head Terms;
ii. where relevant, the risk profile of the industry participant;
iii. the importance of protecting and promoting human rights online, including the right to freedom of expression, the right not to be subjected to arbitrary or unlawful interference with privacy, the right to protection from exploitation, violence and abuse, and the rights and best interests of children, including associated statutory obligations;
iv. the product or service in question, including its function, purpose, size/scale and maturity as well as the capacity and capabilities of the industry participant providing the product or service; and
v. other considerations set out in this Code.

Class 1A material: is a subcategory of class 1 material used for the purpose of the Code, comprised of child sexual exploitation material, pro-terror material, and extreme crime and violence material,.

Class 1B material: is a subcategory of class 1 material used for the purpose of the Code, comprised of crime and violence material and drug-related material.

End-user: means a natural person in Australia who is an end-user of a product or online service covered by this Code.

FFF: Family Friendly Filter.

ISP: is an internet service provider.

Online Crisis Protocol; means the Protocol governing ISP blocking under Part 8 of the OSA.

OSA: means the Online Safety Act 2021

New Rules

Who do they apply to?

The Code only applies to retail ISPs that supply internet carriage services to end-users, including both mobile and fixed broadband services.

This Code refers to Schedule 4 only. Other schedules may apply to your business if you provide other Internet related services.

What are the new rules?

MCM 1: Inform end users who produce online material of their legal obligations in relation to that material

An ISP must inform its end-users that they must not produce online material that breaches any Australian State,Territory, or Commonwealth law, including the OSA.

This can be achieved by providing information on your website, or within your contractual terms, fair-use or acceptable use policies.

MCM 2: Notify hosting service providers of alleged class 1A material being hosted by the hosting provider

An ISP must notify a hosting service provider within 3 business days if the ISP becomes aware that the hosting service provider is hosting alleged class 1A material.

This notification requirement will only apply if the ISP is aware of the identity and email address of the hosting service provider. However, the ISP must take reasonable steps to identify and obtain the email address of the hosting service provider.

This can be achieved by informing relevant staff of the notification requirement and documenting the relevant team(s) responsible for notifying the hosting service provider..

New Rules

What are the new rules?

MCM 3: Join the Online Crisis Protocol to govern the blocking of certain class 1A material

Upon request by eSafety, an ISP must join (and sign) the Online Crisis Protocol governing ISP blocking, and any equivalent successor protocols to the same effect.

MCM 4: Ensure end-users are advised of how to limit access to class 1A and class 1B material

An ISP must make information available and easily accessible to end-users on filtering products and how they can be obtained. The information must be provided at or close to time of sale.

Example: an ISP may choose to provide filter products directly to end-users or can link to information on filters so that end-users can obtain them directly from the filter provider.

MCM 5: Ensure end-users are advised of the FFF program

An ISP must promote the FFF program, either by incorporating information on its own website or by linking to Communications Alliance's webpage containing information on the FFF. If an ISP already provides other suitable program filters, the ISP must also promote the FFF program so that end-users have the option of taking up an FFF.

This can be achieved by the ISP linking the FFF page on promoting the FFF program or certified FFF on its website or in its communications.

New Rules

What are the new rules?

MCM 6: Ensure end-users are informed of their right to make complaints about class 1A and class 1B material to content providers and the Commissioner, and how to do so

An ISP must make information available to end-users about their right to complain to a content provider and eSafety (including where a complaint to a content provider remains unresolved) about class 1A and class 1B material, or electronic messages that promote such material.

This can be achieved by the ISP providing this information, and include a link to the eSafety's website on its website.

MCM 7: Link to eSafety's complaints reporting process

An ISP must make available, via its website, a link to eSafety's online content complaints reporting process.

MCM 8: Responding to complaints

An ISP must either respond to any complaint it receives from an end-user about class 1A or class 1B material, or refer the complainant to eSafety.

New Rules

What are the new rules?

MCM 9: Safety information

An ISP must make plain-language information on online safety regarding class 1A and class 1B material easily accessible to end-users. This includes information for parents/carers about how to supervise and control children's access and exposure to such material, and provide information about the role and functions of the eSafety Commissioner.

An ISP can achieve this by providing its own online safety resources or linking the material on eSafety's website.

MCM 10: Reporting

Where eSafety issues a written request to an ISP to submit a Code report, the provider must, within 2 months of the request submit to eSafety a Code report which includes the following information:

a. the steps that the ISP has taken to comply with their applicable minimum compliance measures;

b. an explanation as to why these measures are appropriate;

c. the number of complaints in relation to class 1A and class 1B material an ISP has responded to under minimum compliance measure 8 above; and

d. the number of complaints received about compliance with this Code.

An ISP will not be required to submit a Code report to eSafety more than once in any 12-month period.

Refer to glossary definition for 'appropriate'.

What This Means For You

Changes to policy often means changes for you and your business.

Employee training in online safety and minimum compliance measures.

Maintain record keeping processes.

Potentially update website and communications material.

Publish relevant advice regarding online safety on website.

Helpful Information

Regulation can be difficult to understand, so talk to people who can help!

Contacts:

Internet Association of Australia Ltd
02 9037 6404
policy@internet.asn.au
www.internet.asn.au

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

Online Safety
https://onlinesafety.org.au/codes/

Read the Code:

Head Terms
applies to all Internet sections

Schedule 4 - Internet Carriage Services Code