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

DRAFT

1 Structure

This Code is comprised of the terms of this Schedule together with the Online Safety Code (Class 1A and Class 1B Material) Head Terms (**Head Terms**).

2 Scope

This Code applies to providers of internet carriage services (**internet service providers** or **ISPs**), so far as those services are provided to customers in Australia.

This Code only applies to **retail ISPs**, that means entities that supply internet carriage services to Australian end-users.

Note: retail internet carriage services include both mobile and broadband services.

3 Definitions

Unless otherwise indicated, terms used in this Code have the meanings given in the OSA or in the Head Terms or as set out below.

Filter means capability designed to limit access to certain types of material, including Class 1A and 1B material, on the internet

Plain language means the use of simple, clear and straightforward language. Plain language simplifies complex ideas for easy understanding. It avoids complicated words and keeps sentences short. It allows for inclusive and efficient communication. It makes information easier to retain.

Note: Consumers are more likely to engage with information that is presented in a straightforward and understandable manner. Plain language is particularly important when communicating with a diverse audience or when conveying important information, by reducing the risk of misinterpretation or confusion. It is especially important for effective communication with consumer with English as a second language, as well as those with disabilities or learning difficulties – the goal is to communicate in a way the average 12-14 year-old would be able to understand.

4 Role of internet service providers

(a) Internet service providers enable end-users to access the internet. They provide the physical or virtual infrastructure for connection to the internet, and associated routing services.

(b) Internet service providers do not engage in any of the following:

(i) hosting of user-generated content;

(ii) allowing end-users to link to, or interact with, other end-users on the service (for example, via video calls, live streaming, chat services). An internet carriage service merely consists of the connection to the internet rather than any voice call, email service, text or chat service that may be transmitted over that service – providers of such services will be subject to other industry codes or applicable industry standards made under the OSA; or

(iii) allowing end-users to generate, store, post or share material on the service (for example, via content upload and file sharing).

(c) Consequently, internet service providers cannot control the content accessible using their services. The only way to potentially limit access to material accessible using their service is (in some cases) through blocking access to content on a domain basis.

Note: eSafety can request and/or direct internet service providers to block material that promotes, incites, instructs in or is material that depicts abhorrent violent conduct in accordance with Part 8, Divisions 2 and 3

of the OSA. Such material would often also be likely to fall under class 1A or class 1B material. However, eSafety does not have powers under the OSA to direct internet service providers to block other class 1A or class 1B material that does not promote, incite, instruct in or is material that depicts abhorrent violent conduct.

(d) Internet service providers are distinct from providers of hosting service, relevant electronic services, designated internet services and/or content providers. They may provide one or more of these services in addition to providing internet carriage services; however, where this is the case, these services would be subject to the other industry codes or applicable industry standards made under the OSA instead of this Code.

For example: An internet service provider that also provides a third-party hosting service will be subject to this Code for its internet carriage services and will be subject to the Hosting Services Online Safety Code (Class 1A and Class 1B Material) or other applicable industry standard for the third-party hosting services it provides.

5 Risk profile

While there are different types of retail internet carriage services (e.g. fixed line, mobile), for the purpose of this Code and the compliance measures in this Code, retail internet carriage services are deemed to have a generally equivalent risk profile. As such, minimum compliance measures under this Code apply to all retail internet services providers.

~~5~~6 Compliance measures

The table in clause ~~7~~6 below contains minimum compliance measures for internet service providers that are subject to this Code.

The table in clause ~~7~~6 also sets out guidance on the implementation of some measures. The guidance and notes are not intended to be binding but are rather provided to provide further guidance on the way that a relevant industry participant may choose to implement a measure.

~~6~~7 Compliance measures for class 1A and 1B material

Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.	
Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material. &	
Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.	
Minimum compliance measures for all Internet Service Providers	**1) Informing end users who produce online material of their legal obligations in relation to that material** An internet service provider must inform its Australian end-users that they must not produce online material that is in contravention of any Australian State, Territory, or Commonwealth law, including the OSA. ***Guidance:*** *For example, an internet service provider can achieve this by providing information on the internet service provider's website, or including it within:* *a) sign-up terms of use;* *b) contractual terms;* *c) fair use policies; or* *d) acceptable use policies.*
Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.	
	This outcome is not applicable to internet service providers. Where an internet service provider is also offering third-party hosting services, these services are subject to the Hosting Services Online Safety Code (Class 1A and Class 1B Material).
Outcome 5: Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.	
Minimum compliance measure for all Internet Service Providers	**2) Notifying hosting service providers if the internet service provider becomes aware of alleged class 1A material being hosted** An internet service provider must notify a hosting service provider within 3 business days if the internet service provider becomes aware that the hosting service provider is hosting alleged class 1A material. This notification requirement will only apply if the internet service provider is aware of the identity and email address of the hosting service provider. However, an internet service provider must take reasonable steps to identify and obtain the email address of the hosting service provider. ***Guidance:*** *For example, an internet service provider can achieve this outcome by:* *a) informing relevant staff of the notification requirement; and* *b) documenting the relevant team(s) responsible for notifying the hosting service provider.*

Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.	
Minimum compliance measure for all Internet Service Providers	**3) Joining the Online Crisis Protocol to govern the blocking of certain class 1A material** Upon request by eSafety, an internet service provider must join (and sign) the *Protocol governing ISP blocking under Part 8 of the Online Safety Act 2021 (No.3)* (Online Crisis Protocol) and engage on equivalent successor protocols to the same effect. Note: For avoidance of doubt, the *Protocol governing ISP blocking under Part 8 of the Online Safety Act 2021 (No. 3)* (Online Crisis Protocol) is the version applicable at the time of Code registration.
Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.	
Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.	
Minimum compliance measures for all Internet Service Providers	**4) Ensuring Australian end-users are advised of how to limit access to class 1A and class 1B material:** An internet service provider must make information available to Australian end-users on filtering products, ~~and~~ how they can be obtained and how end-users can provide feedback about compatibility issues between the filtering product and the internet service provided by the internet service provider. This information must be easily accessible on an internet service provider's website (if the internet services provider has a website), in plain language and be provided at or close to the time of the sale, as well as at least annually thereafter. ***Guidance:*** *For example, an internet service provider may choose to provide filter products directly to their Australian end-users or can link to information on filters so that Australian end-users can purchase them directly from the filter provider.* *End-users may experience compatibility issues between their filtering products and the operating system, other software or settings on their devices, including malware detection software. These issues are not within the internet service provider's responsibility and/or control, and internet service providers are unlikely to be able to assist with these issues.* **5) Ensuring Australian end-users are advised of the Family Friendly Filter (FFF) program** When providing the information as required in measure 4, ~~A~~an internet service provider must promote the ~~Communications~~ Australian Telecommunications Alliance FFF program, either by incorporating information on its own website or by linking to an ~~Communications~~ Australian Telecommunications Alliance page that contains this information. If an internet service provider already provides non-FFF program filters, the provision of those filters will not be impacted, but internet service providers must also promote the FFF program so that Australian end-users have the option of taking up an FFF. ***Guidance:*** *For example, an internet service provider can link to the FFF page on the Communications Alliance website which provides information on, and links to, various FFF providers. ISPs should also promote the Family Friendly Filter program and certified FFF on their websites or in relevant communications to Australian end-users.*
Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.	

Minimum compliance measures for all Internet Service Providers	**6) Ensuring Australian end-users are informed of their right to make complaints about class 1A and class 1B material to content providers and the Commissioner, and the procedures for doing so** An internet service provider must make available information to Australian end-users on 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 unsolicited electronic messages that promote such material. ***Guidance:*** *For example, this should be done via an internet service provider's website and should include a link to eSafety's website.* **7) Linking to eSafety's complaints reporting process** An internet service provider must make available, via its website, a link to eSafety's online content complaints reporting process.
Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and class 1B material.	
Minimum compliance measure for all Internet Service Providers	**8) Responding to complaints** An internet service provider must either establish processes, procedures and/or systems to respond to any complaint or report it receives from an Australian end-user about class 1A and class 1B material or refer the complainant/reporter to eSafety. An internet service provider's process to respond to a complaint or report about class 1A and class 1B material must be easily accessible, easy to use and include or be accompanied by clear instructions on how to use the process. An internet service provider must respond to the complaint or report in a timely manner, including where the provider refers the complainant/reporter to eSafety.
Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.	
Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.	
Minimum compliance measure for all Internet Service Providers	**9) Safety information** An internet service provider must make easily accessible to Australian end-users plain-language information on online safety in respect of class 1A and class 1B material, including information for parents/carers about how to supervise and control children's access and exposure to class 1A and class 1B material, and provide Australian-end-users information about the role and functions of the eSafety Commissioner. ***Guidance:*** *For example, an internet service provider can achieve this outcome by:* *a) providing its own online safety resources; or* *b) linking to material on eSafety's website.* *An internet service provider could provide the links or information through any of its usual communication channels.*
Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.	
Minimum compliance measure for all Internet Service Providers	**10) Reporting** Where eSafety issues a written request to a provider of an internet service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: a) the steps that the provider 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 internet service provider has responded to under minimum compliance measure 8 above; and d) the number of complaints received about compliance with this Code. A provider of an internet service who has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of an internet service will not be required to submit a Code report to eSafety more than once in any 12-month period. Note: 'appropriate' has the meaning given in the Head Terms.