Schedule 5 – App Distribution Services Online Safety Code (Class 1A and Class 1B Material)

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

(a) This Code only applies to app distribution service providers to the extent that they provide a service that enables the download of third-party apps by Australian end-users.

(b) This Code does not apply to an app distribution service provider to the extent that it provides first-party apps.

For example**:** If an app distribution service provider provides an app distribution service that distributes third-party apps and first-party apps this Code will only apply to the extent that the app distribution service enables the download of third-party apps.

(c) This is because the app distribution service provider will also be the app provider for the purposes of a first-party app, and other industry codes made under the OSA will apply to them in their role as the app provider.

For example: An app provider that provides a relevant electronic service via an app will be subject to the Relevant Electronic Services Online Safety Code (Class 1A and Class 1B Material).

For example: An app provider that provides a designated internet service via an app will be subject to the Designated Internet Services Online Safety Code (Class 1A and Class 1B Material).

(d) This Code does not apply where the provider of an app distribution service is an enterprise or other organisation (e.g., a business, public sector, government, or not-for-profit organisation) that exclusively distributes apps for internal use by the enterprise or organisation for the enterprise or organisation's stated purpose (e.g., following approval from the organisation's information technology department).

(e) A person does not provide an app distribution service merely because:

(i) the person supplies a carriage service that enables apps to be downloaded; or

(ii) the person provides a billing service, or a fee collection service, in relation to a social media service, relevant electronic service, designated internet service or app distribution service.

(f) The provider of an app distribution service that exclusively distributes third-party apps of the kind described in clause 4(c)(i) that have been classified by the National Classification Scheme is not subject to this Code.

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.

App includes a computer program.

App distribution service means a service that enables end-users to download apps, where the download of the apps is by means of a carriage service.

App distribution service provider means a person who provides an app distribution service.

App provider means a person who provides an app.

first-party app is an app that is provided by the same person who also provides an app distribution service in relation to that app.

third-party app is an app that is:

(a) provided by a person other than the app distribution service provider for that app; and

(b) standalone in nature (i.e., not separate components of a program).

Note: Third-party apps do not include first-party apps because third-party apps are developed or made by a person other than the app distribution service provider.

third-party app provider means an app provider who:

(a) contracts with an app distribution service provider; and

(b) provides a-third-party app to the app distribution service provider,

for distribution of the third-party app on the app distribution service provider's app distribution service.

4 Role of app distribution service providers

(a) App distribution services permit end-users to easily browse apps from multiple app providers and assist app providers to reach and distribute their apps to a broad range of potential end-users.

(b) App distribution service providers receive apps from third-party app providers for placement on their app distribution services and distribute such apps to end-users. However, once an end-user installs a third-party app, that app may enable the end-user to access content provided by the third-party app provider or other third-party source(s) (including user-generated content) rather than via the app distribution service provider.

(c) Apps generally fall into a number of categories such as:

(i) simple apps that are self-contained software and do not involve any user generated content or interactivity (for example, an app that allows a user to play chess may be entirely self-contained) – for such apps, the content that will be available to the end-user is often visible to the app distribution service provider from the app software provided to it.

(ii) apps that are partially self-contained software (i.e. some content is "embedded" and is visible to the app distribution service provider from the software provided to it) but where other content is "pulled" from other sources once the end-user has downloaded the app and starts to use it (for example, a weather app) – for such apps, the content "pulled" from other sources after download is not visible to the app distribution service provider from the app software provided to it; and

(iii) apps that are software which largely operate as structures or pipelines through which content from other sources (including user-generated content) will be provided or shared – for such apps, such content will not be visible to the app distribution service provider from the app software provided to it.

(d) An app distribution service provider does not directly control or have visibility of all content shared via third-party apps distributed via the provider's app distribution service and cannot take direct action to prevent access or exposure by Australian end-users to class 1A and class 1B materials via such apps.

(e) The measures in this Code are designed to be proportionate to the capacity of app distribution service providers to mitigate risks to Australian end-users relating to class 1A and class 1B materials that may be accessible to Australian end-users via third-party apps – primarily through their engagement with third-party app providers and through the provision of information to Australian end-users that supports safe use of apps distributed via an app distribution service.

5 Compliance measures

The table in clause 6 below contains minimum and optional compliance measures for providers of app distribution services, so far as those services are provided to Australian end-users.

The table in clause 6 also sets out guidance and notes 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 Compliance measures for class 1A and class 1 B 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.	
Minimum compliance measures for all app distribution services	**1) Engagement with third-party app provider/s** An app distribution service provider must: a. have agreements in place with third-party app providers that require the third-party app provider to comply with applicable Australian content laws and regulations; b. have systems, policies and/or procedures in place that enable an app distribution service provider to enforce the provisions in the agreements referred to in measure 1) a); c. review, to the extent reasonably practicable, third-party apps that may be provided to Australian end-users via the app distribution service provider before those third-party apps are released on the app distribution service; and d. take steps to ensure all third-party app providers are made aware of other industry codes made under the OSA that may apply to them in their role as the app provider. ***Guidance:*** *The main ways that app distribution service providers can contribute to Outcome 1 is to put in place agreements with third-party app providers that include provisions concerning the regulatory obligations of the third-party app providers to prevent, or limit the accessibility of, or exposure to, class 1A or class 1B materials for Australian end-users via third-party apps distributed on an app distribution service; and to have processes and systems in place that enable the provider to enforce agreements. For example, an app distribution service provider may include provisions in agreements with app providers that:* *i. require the app provider to take steps to prevent or limit any material or activity (as relevant) that breaches applicable Australian content laws and regulations from being created, shared, hosted, or facilitated via third-party apps it distributes on the app distribution service;* *ii. require the app provider to ensure apps distributed via the app distribution service are not designed to facilitate activity that breaches applicable Australian content laws and regulations;* *iii. permit the app distribution service provider to suspend or remove a third-party app from the app distribution service in appropriate circumstances (such as removal on receipt of an app removal notice from eSafety under the OSA);* *iv. require third-party apps and updates to undergo a review process before being released on the app distribution service; and/or* *v. permit the provider to reject or require changes to apps that do not pass a review in iv).* *Any enforcement action should be proportionate to the nature of the provider's breach of the agreement.* ***Note**: For the purpose of sub-measure 1 a) applicable Australian content laws and regulations include any applicable industry codes or standards made pursuant to the OSA that create legal obligations on third-party providers relating to class 1A and class 1B materials that may be accessible to Australian end-users via an app.*

	2) Trust and safety function An app distribution service provider must ensure that it is reasonably resourced with personnel to oversee the safety of the app distribution service. Such personnel must have clearly defined roles and responsibilities, including for the operationalisation and evaluation of the systems and processes required under this Code. ***Guidance:*** *A trust and safety function should be allocated to one or more employees or external third-party service providers. Some industry participants may rely on the risk management systems of a related entity to assist with complying with this obligation.*
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 measure for all app distribution services	**3) Age and/or content ratings** An app distribution service provider must make age and/or content ratings information about third-party apps available on the app distribution service to Australian end-users at the time those third-party apps are released on the app distribution service. ***Guidance:*** *An app distribution service provider may either undertake its own age and/or content rating processes for third-party apps or may require third-party app providers to undertake an age and/or content rating process (which may be through an external ratings authority) and to provide the outcome of that rating process to the app distribution service provider.* *If an app distribution service provider establishes its own age and/or content rating process, the app distribution service provider should consider (i) the appropriateness of the features of the app for children, including whether the app is developmentally appropriate for children, taking into account whether the app provides access to user-generated content or enables users to create and share still images or video; and (ii) whether features of the app will likely expose end-users to sex, violence or strong language.*
Outcome 4: Industry participants take reasonable and proactive steps to prevent or limit hosting of class 1A or class 1B material in Australia.	
No compliance measure for app distribution services	This Outcome is not applicable to app distribution service providers.
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 app distribution services	**4) Industry forum** An app distribution service provider must take part in an annual forum organised or facilitated by any industry association referred to in the Head Terms to discuss and evaluate the effectiveness of measures in this Code and share best practice in implementing this Code and online safety in general with other industry participants.

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 app distribution services	**5) Technological updates** An app distribution service provider must share information with eSafety about significant new features or functions released by the app distribution service provider that the app distribution service provider reasonably considers are likely to have a significant effect on the access or exposure to, distribution of, and online storage of class 1A or class 1B materials in Australia. In implementing this measure, industry participants are not required to disclose information to eSafety that is confidential.
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 measure for all app distribution services	**6) Online safety resources** An app distribution service provider must provide online safety resources that include clear and accessible information for Australian end-users regarding: a) the age and/or content ratings approach used by the app distribution service provider pursuant to measure 3; b) steps that parents and guardians may take to supervise and manage children's use of apps; c) information about the ability of Australian end-users to report or complain about content on a third-party app to the third-party app provider (being information that can help Australian end-users to report or complain about class 1A or class 1B material); d) information about the mechanisms in measure 7; and e) the role and functions of eSafety, including how to make a complaint to eSafety.
Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.	
Minimum compliance measure for all app distribution services	**7) Enabling reporting by end-users** An app distribution service provider must provide a mechanism that enables Australian end-users to report or make a complaint about: a) a failure by a third-party app provider to satisfactorily resolve a report or a complaint by the Australian end-user concerning class 1A or class 1B material on a third-party app distributed by the app distribution service provider; and b) a breach of this Code by the app distribution service provider. The reporting tool and complaints mechanism must: c) be easily accessible and easy to use; and d) be accompanied by plain language instructions on how to use it, as well as an overview of the reporting process. An app distribution service provider must respond within a reasonable timeframe to complaints concerning class1A or class1 B materials that are lodged by an Australian end-user. ***Guidance:*** *An Australian end-user may be required by the app distribution service provider to report class 1A and class 1B material on an app directly to the relevant third-party app provider, as a condition of making a report or complaint under sub-measure 7*

	a) and should in any case be encouraged to reach out to the relevant third-party app provider in the first instance *The app distribution service need not provide an on-platform tool for the purpose of complying with this measure and may for example implement this measure by providing an Australian end-user with access to a web site, chat function, email address, or hotline.*
Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and class 1B material.	
Minimum compliance measure for all app distribution services	By complying with the minimum compliance measures under Outcome 8, app distribution service providers will also meet the requirements of this Outcome.
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 app distribution services	By complying with the minimum compliance measures under Outcome 7, app distribution service providers will also meet the requirements of this Outcome.
Outcome 11: Industry participants publish annual reports about class 1A and class 1B material and their compliance with this Code.	
Minimum compliance measure for all app distribution services	**8) Reporting by providers of app distribution services** Where eSafety issues a written request to a provider of an app distribution 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; and b) an explanation as to why these measures are appropriate. A provider of an app distribution service who has received such a request from eSafety is required to submit a Code report within 6 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 app distribution 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.