ONLINE CRIMINAL HARMS ACT 2023
CODE OF PRACTICE FOR ONLINE MESSAGING AND CONFERENCING SERVICES
(with effect from 17 August 2026)

1. This Code of Practice is issued pursuant to section 21(1)(*b*) of the Online Criminal Harms Act 2023 (the "**Act**") and applies to all providers of Online Messaging and Conferencing Services[1] ("**Designated Providers**").

2. This Code of Practice aims to:

   (a) enable the quick disruption malicious accounts and activities;
   (b) put in place safeguards to prevent propagation of malicious activities; and
   (c) ensure accountability.

3. It will come into operation on 17 August 2026.

4. All Designated Providers must take all reasonable steps to comply with this Code of Practice, including but not limited to implementing appropriate systems, processes or measures to counter and prevent the use of their designated online service(s) for the commission of scams and/or malicious cyber activity offences specified in the Second Schedule to the Act.

Requirements

5. Unless otherwise informed by the Competent Authority, all Designated Providers must implement the appropriate systems, processes and/or measures within the periods specified below, as calculated from the date of application of this Code of Practice as stated in the Code Application Notice that is issued to you:

   a. Section A: six (6) months;
   b. Section B: six (6) months;
   c. Section C (except C5): six (6) months;
   d. Section D (except D1): six (6) months;
   e. Section E: six (6) months; and
   f. C5 and D1: two (2) months.

[1] Online messaging and conferencing service means any online service that enables end user(s) to communicate (including but not limited to the sharing of information) with other end user(s), through text, voice, images, video or multi-media communications, whether on a one-to-one, one-to-many or group basis, including through messaging, calling, conferencing, group or any other channel functionalities. A "designated online messaging and conferencing service" means an online service that has been designated under s20(1) of the Act.

Section A – Proactive Detection of Malicious Accounts and Activities

A1)	Proactively detect and promptly take all necessary actions[2] against suspected scams and/or malicious cyber activities, as well as accounts which are used to commit or facilitate them, including compromised, inauthentic or bot[3]-controlled accounts.
A2)	Proactively detect and promptly remove, or prevent the publication of: (a) content containing images, videos, audios, likeness, or other representations that impersonate a public figure, brand or business with a 'verified' account, and the accounts that facilitate the communication of such content; and/or (b) accounts that impersonate a public figure, brand or business with a 'verified' account.
A3)	Put in place an easily accessible reporting mechanism to allow Singapore end-users to report suspected scams and/or malicious cyber activities (including but not limited to compromised end-user accounts, and accounts that impersonate the end-users) that occur or are suspected to occur through end-user accounts. Designated Providers shall promptly assess and take the appropriate action(s)[4] on such reports, within 24 hours of receipt of the report, or otherwise informed by the Competent Authority
A4)	Identify trending or changing behaviour associated with scams or malicious cyber activities (e.g. from end-user reports received or information received from law enforcement agencies), and promptly update the fraud analytics accordingly with new and changing trends or behaviour.
A5)	Implement a fast-track channel to receive reports from law enforcement agencies in Singapore relating to trends (e.g. the trending *modus operandi*, scam types etc.) on scams and/or malicious cyber activities[5]. Designated Providers shall act on the reports promptly and update the agencies expeditiously on the (i) specific measures taken or to be taken to detect, prevent and minimise the occurrence of similar activities; and (ii) implementation timeline of such measures.
A6)	Screen advertisements[10] for suspicious[6] content and regularly monitor embedded URLs to check if the URLs change during the lifecycle of the advertisements.

[2]Actions to be taken include, but are not limited to reviewing, investigating, verifying, warning, suspending, restricting the account(s) that are suspected to be used to commit or facilitate scams and/or malicious cyber activities, with the outcome of disrupting such activities.

[3]"Bot" means a computer program made or altered for the purpose of running automated tasks.

[4]Actions to be taken include, but are not limited to warning, suspending, or restricting the scams and/or malicious cyber activities, and accounts used to commit or facilitate them, with the outcome of disrupting the scams and/or malicious cyber activities.

[5] Such reports may include information on trends or modalities of scams and/or malicious cyber activities

[6] Suspicious content refers to content within an advertisement that may be indicative of scams or malicious cyber activities, including but not limited to: (a) unrealistic promises of financial returns or gains; (b) impersonation of legitimate businesses, brands or public figures; (c) URLs that redirect end-users to unverified or fraudulent websites; (d)

A7)	Identify and assess the legitimacy of an advertisement[10] when it has adopted URL cloaking to hide a destination website's URL.
A8)	Review all advertisements that are intended to be accessible to Singapore end-users before the publication such advertisements and prevent the publication of any such advertisement to be accessible to Singapore end-users if there is reason to suspect that the advertisement is in furtherance of a scam and/or malicious cyber activity, based on information known to the designated online service provider at before the time of publication.

Section B – Verification Measures

B1)	Put in place reasonable verification measures to prevent the creation and usage of inauthentic, bot-controlled or compromised accounts for scams and/or malicious cyber activities.
B2)	Conduct additional verification procedures on an account when there is detection of suspicious conduct or activity by the account as reported by Police, end-users, and/or Designated Provider's/ Service's detection mechanism.
B3)	Require holders of accounts to have in place login verification features that provides effective protection against unauthorised access. Strongly encourage end-users to adopt enhanced security measures including multi-factor authentication, biometric verification or other forms of authentication measures available on the online service.
B4)	Require consent from the account holder before permitting a login from a new or unrecognised device.
B5)	Provide account holders with the option to designate their accounts as 'verified', that comes with stronger verification or authentication measures[7]. Inform end-users that 'verified' accounts are more likely to be authentic and more reliable, and inform end-users of the process and criteria for obtaining such status.
B6)	Verify the identities of advertisers[8] by conducting checks against Government-issued records including but not limited to business registration records and

high-pressure tactics to solicit personal or financial information; or (e) promotion of unlicensed financial products or services.

[7] Such stronger measures include and are not limited to conducting checks against government issued records or other reliable information to confirm the authenticity of the account.

[8] An "advertiser" refers to any person or entity that directly or indirectly creates, publishes, promotes, pays for, authorises, or otherwise causes the dissemination of an advertisement, through an online service, whether for its own benefit or for the benefit of another person or entity. This includes but is not limited to a brand owner, merchant, advertising or marketing agency, public relations agency, content creator, influencer, affiliate marketer, or any other intermediary involved in the creation, targeting, placement, promotion, funding or dissemination of the advertisement.

	identification documents where applicable, before they are permitted to publish any advertisements.

Section C – Account and User Protection Measures

C1)	Require an end-user to consent before the end-user can be added into a chat group, channel or similar group communication function by an unknown account.
C2)	Provide end-users with the option to silence, filter[9] or block messages or calls originating from accounts or telephone numbers that are not present in the end-users' contact list, and apply the end-user's selected option as the default setting until the end-user changes that setting
C3)	Provide appropriate safeguards and user protection measures where end-users receive direct messages, calls or communications from unknown or suspicious accounts, including displaying contextual warnings or risk indicators and enabling end-users to silence, filter, reject, control or block such communications.
C4)	Provide end-users with contextual account information relating to accounts not present in the end-user's contact list, including, where applicable, the account creation date, account age, country or region associated with the account's registration or origin, to enable end-users to make informed decisions on whether to engage or continue communications with such accounts.
C5)	When an end-user receives a message, call or other communication from an account that is not present in the end-user's contact list or an account that meets conditions specified by the Competent Authority, the account identifier, including the telephone number where applicable, profile name, display name, profile picture and/or any other user-selected identifier associated with that account, must be displayed, or omitted from display, in such manner as may be specified by the Competent Authority. Such display, or omission of display, shall remain in effect until the end-user saves the account as a contact or otherwise designates the account as a known contact.
C6)	Implement limits on the number of end-users who can join or follow a channel or similar broadcast communication function, except for channels or similar broadcast communication functions that are created by end-users who have been subjected to stronger account verification or authentication measures and are authorised to create, administer, post, publish, edit or manage content within such channel or broadcast function.
C7)	Where suspicious conduct or activity is detected in relation to an account of an end-user, implement restrictions on the end-user's ability to initiate new conversations, chats, calls or communication sessions, create and manage chat

[9] 'Silence' refers to the muting of notifications from such accounts or telephone numbers, and 'filter' refers to the automatic redirection of messages from such accounts or telephone numbers to a separate folder or inbox.

	groups, channels or similar group communication functions, including restrictions on: (a) the number of chat groups, channels or functions that may be created; and (b) the number of end-users that may be added or invited to such chat groups, channels or functions. (c) the number of new conversations, chats, calls or communication sessions that end-user may initiate within a specified period.

Section D – Disabling of Malicious Accounts and Activities

D1)	Prohibit or otherwise limit communication functions specified by the Competent Authority (e.g. users, chat groups, channels) from using profile names, display names, usernames, email prefixes, profile pictures or logos that are prohibited in the list as provided by the Competent Authority. This list includes, but is not limited to, names, numbers or logos of government trusted communication channels and government agencies, or any of their homoglyphs.
D2)	Where suspicious conduct or activity is detected in relation to a channel/similar broadcast communication function or any associated owner, administrator or moderator, implement stronger enforcement measures, for instance, suspension, disabling, access restriction, or banning of the relevant channel or accounts associated with suspected scams or malicious cyber activities.
D3)	For advertisements that have been published and are accessible to Singapore end- users, to remove the advertisements promptly when there is reason to suspect that the advertisement is in furtherance of a scam and/or malicious cyber activity.
D4)	Disallow the publication of advertisements[10] offering financial services and/or products to Singapore end-users unless the advertisers[9] are licensed by the Monetary Authority of Singapore (MAS) or other applicable Singapore authorities or are authorised by a licensed entity, to do so in Singapore.

Section E – Reporting and Accountability Requirements

E1)	Inform the relevant law enforcement agencies expeditiously of any detected trends or modalities of scams and/or malicious cyber activities occurring on the

[10] "Advertisements" means content communicated by the Designated Provider on its online service as part of a service provided by the Designated Provider in exchange for the payment of money or any value.

	designated services and provide relevant associated information, and the actions that have been taken to address them.
E2)	Retain all available data of accounts reported or assessed as being used or having been used for scams and/or malicious cyber activities based on information provided by the Police[11], such as records that identify the user(s) of the account, records of transactions or interactions, activity logs, IP addresses and metadata, for a minimum of 90 days from the date of the designated provider is informed of the account in question in order to facilitate potential criminal investigation into the scams and/or malicious cyber activities.
E3)	Maintain and preserve any such records requested by law enforcement agencies for criminal investigations into scams and/or malicious cyber activities for as long as is deemed necessary by the law enforcement agencies.
E4)	Facilitate requests for information and data from law enforcement agencies, including putting in place expedited channels for emergency requests.
E5)	Submit to the Competent Authority an annual report on the implementation of the systems, processes and measures to counter and prevent online scams and/or malicious cyber activities covered in sections A, B, C, D and E, in accordance with the timeline as stated in the Code Application Notice that is issued to the Designated Providers, or unless otherwise informed by the Competent Authority. The report shall include, but is not limited to the following information: i. Descriptions of existing and newly implemented policies, programs, systems, techniques, processes and measures implemented to detect, prevent and respond to scams and/or malicious cyber activities on the online service(s). ii. New challenges observed in countering and preventing scams and/or malicious cyber activities on the online service(s), such as changes in tactics employed by malicious actors. iii. Measures being explored or developed to improve existing systems and techniques to detect, prevent and respond to scams and/or malicious cyber activities on the online service(s). iv. Suitable metrics and information, proposed by the Designated Providers and subject to the agreement by the Competent Authority, on the effectiveness of the implemented measures. This includes, but is not limited to the following: a) Number of accounts/ contents associated with scams and/or malicious cyber activities, proactively detected and removed or banned; and

[11] This refers to information provided by the Police either via the OCHA directions or provided by the Police for designated provider's assessment if there is any violation of their terms of service, policy and/or guidelines, etc.

	b) Number of Singapore end-user reports received, number of Singapore end-user reports on which actions were taken, and time taken to take action from the moment of receipt of Singapore end-user reports.