

Public Consultation Paper on Enhancing Online Safety: Empowering Singaporeans to Seek Relief from Harmful Online Content and Conduct, and Hold Responsible Parties Accountable

Contents

I.	Introduction	2
A.	Creating a safer and more inclusive online space.....	2
B.	Approaches to regulation of online harms	3
C.	Limitations of existing laws	3
II.	Proposals to enhance online safety	4
A.	New complaints mechanism.....	4
B.	New statutory torts.....	7
C.	Increasing accountability through improved user information disclosure	8
III.	Submission of Feedback.....	8
	Annex A: Enhancements to the regulatory and criminal framework	9
	Annex B: Study by SG Her Empowerment on online harms in 2023	10
	Annex C: Description of proposed categories of online harm	11
	Annex D: Parties against whom directions may be issued.....	14
	Annex E: Directions which the Agency may make	15
	Annex F: Duties owed by parties under the statutory torts	17

I. Introduction

1. The Ministry of Law (MinLaw) and the Ministry of Digital Development and Information (MDDI) propose a suite of new measures to help victims of online harms and improve accountability of those who are responsible for these online harms. These proposals will complement our existing regulatory frameworks and the criminal justice system.
- A. Creating a safer and more inclusive online space
2. The Internet has transformed how people live, work and play, and become an indispensable part of the daily lives of Singaporeans.¹
3. At the same time, many are concerned about the harmful aspects of the Internet. The Internet can be used to host and quickly distribute harmful online content, such as child abuse material or material promoting self-harm. The Internet has also been misused for criminal activities, such as scams and the sale of contraband, and to spread misinformation.
4. The Government has recently introduced a series of measures to address various aspects of online harms. We strengthened our ability to act against online criminal harms under the Online Criminal Harms Act. We also introduced the Online Safety (Miscellaneous Amendments) Act 2022 which amended the Broadcasting Act 1994 (“**BA**”) to impose greater regulatory requirements on online communication services. Further, some forms of online harassment are addressed through the Protection from Harassment Act 2014 (“**POHA**”) (see Annex A). These are on top of public education efforts such as the creation of the Media Literacy Council, and the teaching of Internet safety in schools.
5. Despite these efforts, a 2023 survey conducted by SG Her Empowerment (“**SHE study**”) (see Annex B) found that about three in five (58%) respondents in Singapore had personally experienced and/or knew others who faced online harms.² A 2024 survey conducted by MDDI found that about three in four (74%) respondents encountered harmful content such as cyberbullying or sexual content online, an increase since 2023 (65%).³
6. We are concerned about the impact of online harms on individual victims and society as a whole.⁴ Victims may suffer from consequences such as mental and physical health issues, reputational damage, financial losses, and even physical harm, and develop a fear of speaking out. The SHE study found that about two in five online harms survivors experience serious emotional, mental, or physical impact, such as fearing for their own safety, depression, and self-harm. The study also showed that some retreat from participating online because of online harms. Most become uncomfortable expressing their views on potentially controversial topics online (76%), while a majority self-censor (66%) or disengage (68%) as a form of self-help. These issues are compounded when online harms become normalised, and over time social unity and trust is eroded.

¹ IMDA’s 2022 Annual Survey on Infocomm Usage in Households found that 99% of resident households in Singapore have access to a smartphone. Top uses of the internet included communication, getting information, leisure, and dealing with government and banks.

² See SHE study, pages 9-10.

³ MDDI’s annual Online Safety Poll (conducted in April 2024).

⁴ See SHE study, pages 14-17. See also Safeguarding Online Spaces study by SG Her Empowerment in 2023 (“SOS study”).

7. We are also concerned that online harms may become more pervasive over time, as online anonymity and difficulties in holding wrongdoers accountable for their actions embolden more individuals to post harmful content.

B. Approaches to regulation of online harms

8. Regulating harmful online content requires a balance between protecting victims from harm and respecting individuals' rights to express themselves online.

9. Singapore and other jurisdictions have introduced regulations that focus on requiring platforms to have systems and processes to mitigate and reduce the risks of certain types of harmful online content on their platforms.⁵ In Singapore, designated platforms must comply with Codes of Practice and put in place systems and processes to mitigate risks from exposure to harmful content. While platforms are required to moderate content and activities on their own, a common challenge many jurisdictions face is the lack of transparency in the moderation practices and outcomes in individual cases. Some jurisdictions, such as Australia⁶ and the European Union⁷, also adopt an approach where laws require that harmful content be taken down or addressed.

10. In Singapore, similar to the legal powers of other jurisdictions such as Australia and the European Union, the amended BA also enables the Infocomm Media Development Authority to issue directions to disable access to egregious content on online communication services. Victims of online harms may also take legal action under legislation such as the POHA or traditional legal claims.

C. Limitations of existing laws

11. Our existing regulatory approach seeks to reduce the prevalence of online harms by imposing requirements and standards on online communication services. However, surveys and studies show that online harms still take place and victims continue to suffer from the harms they encounter online.

12. Our review therefore focussed on assessing whether victims are able to (i) quickly and effectively seek relief from harmful online content or conduct and (ii) hold wrongdoers accountable for their actions.

13. Some of the limitations in our existing laws revealed in our review are:

⁵ See for instance, the Online Safety (Miscellaneous Amendments) Act, which took effect from 1 February 2023. With this Act, a new part has been introduced to the Broadcasting Act to regulate Online Communication Services accessible by Singapore users.

⁶ For instance, victims of online harms in Australia can submit a report to the Australian eSafety Commissioner, who will act on the report should it meet the threshold. The eSafety Commissioner investigates cyberbullying of children, adult cyber abuse, image-based abuse (sharing or threatening to share intimate images without the consent of the person shown), and illegal and restricted content.

⁷ The Digital Services Act ("DSA"), which applies across the European Union, requires digital service providers to take action against illegal content. The DSA imposes obligations on certain internet intermediaries, mainly content hosts, to allow users to report illegal content, and expeditiously remove such content upon being notified. Intermediaries may be fined up to 6% of their annual turnover. Very large online platforms and search engines also have obligations to conduct risk assessment and mitigation, crisis response, independent audit, etc.

- a. Challenges of the court process. Most people find court processes intimidating, costly, and difficult to navigate. They prefer to obtain a remedy via a simpler and faster process.⁸
 - b. Existing laws cover a narrow set of online harms. POHA provides relief for harassment and false statements only. The applicability of POHA to other types of online harms such as online impersonation remains mostly untested.
 - c. Victims need to know who the perpetrator is in order to sue them, but getting this information is often difficult or impossible.⁹ Perpetrators hide behind the anonymity offered by the internet and are often not held accountable for their wrongdoings.
14. More must be done to allow victims of online harms to seek help, while also continuing to foster a safe and conducive environment for online discourse.

II. **Proposals to enhance online safety**

15. In summary, we are proposing three key measures as follows:
- a. Introduce a complaints mechanism to provide victims with timely help when faced with online harms;
 - b. Introduce statutory torts, to enable victims to hold responsible parties accountable through liability for online harms; and
 - c. Increase accountability through improved user information disclosure.
- A. New complaints mechanism
16. We propose to introduce a new complaints mechanism, which will be administered by a new Agency. Singapore will be among the first in the world to establish a dedicated Agency to support victims of online harms and enhance online safety. In Australia, the eSafety Commissioner investigates cyberbullying of children, adult cyber abuse, image-based abuse (sharing, or threatening to share, intimate images without the consent of the person shown), and the propagation of illegal and restricted content. Victims of online harms can submit a report to the eSafety Commissioner, who will act on the report if it meets the threshold for action.
17. Likewise, in Singapore, victims¹⁰ of specified types of online harms (see Table 1, with more details in Annex C) or the victims' representatives¹¹ will be able to submit a complaint with the Agency.

⁸ See SHE study, pages 18-19.

⁹ See SHE study, page 19.

¹⁰ Victims allowed to submit a complaint should be Singapore citizens or Permanent Residents, or foreigners with a student's pass, work permit or work visa (including dependents who have the applicable pass). Corporate entities based in Singapore will also be allowed to submit complaints.

¹¹ These include the parents or guardians of victims under 18 years of age, and individuals who have been authorised by the victim in writing to submit a complaint to the Agency on their behalf.

Table 1: Complaints Mechanism - Specified Online Harms

S/N	Online Harm
1.	Online harassment (e.g. cyberbullying, sexual harassment, doxxing and cyberstalking)
2.	Intimate image abuse (i.e. non-consensual sharing of intimate images)
3.	Child abuse material
4.	Impersonation
5.	Misuse of inauthentic material (e.g. deepfakes)
6.	Online statements instigating disproportionate harm or "OSIDH"
7.	Hate speech
8.	Misuse of personal information
9.	False statements (about the complainant)
10.	Statements affecting reputation

18. The new Agency will issue directions to perpetrators, administrators, and online service providers (to be termed communicators, administrators, and platforms respectively) such as social media services to put a stop to the online harm quickly. A description of these parties is summarised below (see more details in [Annex D](#)):
 - a. **Communicator:** Individual or entity who communicated the material that is the subject of a complaint.
 - b. **Administrator:** Individual or entity who creates, sets up or administers an online location.
 - c. **Platforms:** Individual or entity who provides the service by means of which the material complained of had been communicated through the internet (e.g. Facebook, X, TikTok).
19. To illustrate using a given social media page, the person who develops and maintains this page is its administrator, persons who make posts on this page are communicators, while the social media service is the platform.
20. The directions that the Agency can make (depending on the online harm in question) are as follows (more details can be found in [Annex E](#)).

Categories of harm	Directions available against:		
	Communicator	Administrator	Platform
All harms in para 17 except False Statements and Statements Affecting Reputation	<ul style="list-style-type: none"> - Disable access to material by users in Singapore - Labelling, which will require the Communicator to communicate a notice setting out specified instances for which the Communicator has been subject to the Agency's directions 	<ul style="list-style-type: none"> - Disable access to material by users in Singapore - Removal from online group - Closure of online group - Labelling, which will require the Communicator to communicate a notice setting out specified instances for which the Communicator has been subject to the Agency's directions 	<ul style="list-style-type: none"> - Disable access to material by users in Singapore - Deactivation of the Communicator's account - Closure of online group - Engagement reduction
OSIDH, False Statements and Statements Affecting Reputation	Right of Reply	Right of Reply	Right of Reply

21. The Agency will generally first direct that access to the content be disabled or, in the case of false statements or statements affecting reputation, grant the complainant a Right of Reply. The more severe levers will be reserved for more serious cases, for example, if the account is used primarily to perpetuate online harms, or for recalcitrant perpetrators.
22. In deciding on the direction and the recipient of the direction, the Agency may consider factors such as the nature and circumstances of the case, the likelihood of further harm, and any other relevant factors. The Agency may decide not to act in some situations.
23. Recipients of the Agency's directions must comply within a specified time period. In cases where there is non-compliance with an Agency direction, the Agency may take additional measures, such as:¹²
 - a. Access blocking order. This directs internet access service providers to disable access to the online location hosting the harmful content.
 - b. App removal order. This directs app distribution service providers to remove the app containing the harmful content from the app store.

¹² Access blocking and app removal directions issued in respect of non-compliance by a communicator or administrator are available only where there is no platform involved (i.e. where the communicator or administrator runs its own website or app). A platform may be blocked, or have its app removed, only for its own non-compliance with an Agency direction.

24. The Agency will have investigative powers to facilitate its assessment of complaints and may use these powers to gather the facts and information on the circumstances of the cases. The Agency can also investigate non-compliance with its directions as failure to comply will be a criminal offence.

B. New statutory torts

25. We propose introducing statutory torts for specified online harms, to be heard in the Singapore Courts. A tort is a wrongful act or omission that causes harm or injury to another person or their property, leading to civil liability. A statutory tort is a tort that is defined under legislation rather than under common law. This statutory tort proposal clarifies the legal position on the specified online harms listed below, and aims to give victims of online harms more legal certainty should they choose to pursue a claim (e.g. for compensation) in court.

26. The list of online harms covered by the proposed statutory torts is as follows:

Table 2: Statutory Torts Mechanism - Specified Online Harms

S/N	Online Harm
1.	Online harassment
2.	Intimate image abuse
3.	Child abuse material
4.	Impersonation
5.	Misuse of inauthentic material
6.	OSIDHs
7.	Hate speech (for violence-inciting content only)

27. The statutory torts (Table 2) are not intended to cover all of the online harms covered under the complaints mechanism (Table 1). This is to avoid duplicating existing law. For instance, for false statements and statements affecting reputation, a victim could sue in defamation, while for misuse of personal information, a victim could have remedies under existing laws on breach of confidence or breach of contract. For hate speech under the statutory tort, it is restricted to only the most serious forms (i.e. violence-inciting content) so as to avoid over-expansive civil liability.

28. Victims can choose to pursue a claim against communicators, administrators or platforms. The duties of communicators, administrators and platforms are briefly outlined below and more details can be found in Annex F.

- a. Communicator. A person must not communicate and/or publish any specified online harm in Singapore with the intention, knowledge or reasonable grounds to believe that doing so might cause loss or harm to the victim.
- b. Administrator. An administrator must not create, set up or administer an online location in a manner that encourages or increases the risk of specified online harms at the online location. An administrator must also act reasonably to address specified online harms at their online location which they have been notified of.
- c. Platform. A platform must take reasonable measures to address specified online harms which it has been given notice of. Platforms with greater reach and impact will be subject to additional requirements, for example, on the time taken to respond to the user report.

29. A communicator, administrator or platform that breaches its duty under the statutory tort will be liable for the loss or harm suffered by the victim, subject to a defence of reasonable conduct or reasonable excuse.
 30. If a Court finds that a party has breached their duty under the statutory torts, the party may be liable for damages, up to a limit. Further, the Court can make orders that the harm be stopped or be further prevented.
- C. Increasing accountability through improved user information disclosure
31. Finally, we are exploring a proposal to make the user information of perpetrators available to victims who have filed complaints with the Agency. We recognise that online anonymity can be useful as it allows vulnerable persons or groups to speak up without fear of reprisal. However, online anonymity has been exploited by bad actors to target victims without fear of repercussion, and victims who do not know the identity of the perpetrator face difficulties seeking redress. We believe improving accountability will deter perpetrators from committing such harms, and also serve to improve the overall safety of users.
 32. A victim who has filed a complaint with the Agency may apply to the Agency for the disclosure of a perpetrator's user information for certain specified purposes (for example, to bring a claim under the statutory torts or to safeguard themselves from the perpetrator). The Agency may disclose the information to the victim, subject to the victim satisfying prescribed requirements.

III. Submission of Feedback

33. We invite members of the public to provide their feedback on the above proposals by **5pm, 22 December 2024** via the online feedback form at FormSG: <https://go.gov.sg/onlineharmsconsult>. We look forward to your views.

Ministry of Law
Ministry of Digital Development and Information
22 November 2024

Annex A: Enhancements to the regulatory and criminal framework

Regulatory framework

1. The Online Criminal Harms Act 2023 enables authorities to deal more effectively with online activities that are criminal in nature. This includes the issuance of directions by the Police to online services where criminal activities could be conducted, when there is reasonable suspicion that an online activity is being carried out to commit a crime.
2. In 2022, the Broadcasting Act 1994 was amended through the Online Safety (Miscellaneous Amendments) Act to empower the Infocomm Media Development Authority to issue directions to deal with egregious content¹³ communicated on online communication services (OCSs). In addition, designated social media services (SMSs) are required to comply with the Code of Practice for Online Safety, which requires them to put in place measures to mitigate the risks to Singapore users from exposure to harmful content,¹⁴ and provide accountability to users on such measures.

Criminal law framework

3. In 2019, the Penal Code 1871 was amended to better tackle technology-enabled sexual offences. This includes the introduction of specialised offences to criminalise the (i) making, distribution and possession of voyeuristic recordings, intimate images and child abuse material, (ii) distribution of or threat to distribute intimate images or recordings, and (iii) non-consensual exposure of genitals online (i.e. cyber-flashing).
4. In 2019, the Protection from Harassment Act 2014 was amended to strengthen protections for victims of cyberbullying through the criminalisation of doxxing.¹⁵
5. See also paragraph 1 above, on the Online Criminal Harms Act 2023.

¹³ There are seven categories of egregious content defined under s 45D of the Broadcasting Act: (a) content that advocates or instructs on suicide or self-harm; (b) content that advocates or instructs on physical violence against humans; (c) content that advocates or instructs on sexual violence; (d) content that depicts child sexual exploitation; (e) content that poses a public health risk in Singapore; (f) content likely to cause racial or religious disharmony in Singapore; and (g) content that advocates or instructs on terrorism.

¹⁴ Six categories of harmful content were set out in the Code of Practice for Online Safety: (a) sexual content; (b) violent content; (c) cyberbullying content; (d) self-harm content; (e) content endangering public health; and (f) content facilitating vice and organised crime.

¹⁵ POHA, section 3.

Annex B: Study by SG Her Empowerment on online harms in 2023

Link: https://api2.she.org.sg/uploads/SHE_Report_on_Online_Harms_Study_Final.pdf

Annex C: Description of proposed categories of online harm

Category of harm	Description
Online harassment	<p>Threatening, abusive or insulting online behaviour or communication, which is likely to:</p> <ul style="list-style-type: none"> a) cause the victim harassment, alarm, distress or humiliation; b) cause the victim to believe that unlawful violence will be used by any person against the victim or any other person; or c) provoke the use of unlawful violence by the victim or any other person. <p>Includes:</p> <ul style="list-style-type: none"> a) <u>Sexual harassment</u>: Sexual or indecent online behaviour or communication which is likely to cause the victim harassment, alarm, distress or humiliation. b) <u>Cyberstalking</u>: Online conduct involving acts or omissions associated with stalking, which is likely to cause harassment, alarm, distress or humiliation to the victim. c) <u>Doxxing</u>: Online publication¹⁶ of any identity information of the victim and which is likely to: <ul style="list-style-type: none"> a) to be intended to cause the victim harassment, alarm, distress or humiliation; b) cause the victim to believe that unlawful violence will be used by any person against the victim or a related person; or c) facilitate unlawful violence against the victim or a related person.
Intimate image abuse	Online communication ¹⁷ of an intimate image or recording depicting or appearing to depict the victim, without the victim’s consent and which is likely to cause the victim harassment, alarm, distress or humiliation.
Child abuse material	Online communication of child abuse material ¹⁸ depicting the victim. Child abuse material is material which depicts:

¹⁶ “Publication” means to make the communication or statement available in any form such that the communication or statement is or can be heard, seen or otherwise perceived by the public in Singapore or a member of the public in Singapore, and includes cause to be published.

¹⁷ “Communication” here includes distribution, offer or threat to sell or distribute, or advertisement of, the intimate image or recording.

¹⁸ “Material” here includes an offer or threat to sell or distribute, or advertisement of the child abuse material. It excludes material that has a legitimate purpose related to science, medicine, education or art, and does not pose an undue risk of harm to any person below 16 years of age.

Category of harm	Description
	<p>a) a person who is or appears / implied to be below 16 years of age (i) as a victim of torture, cruelty or physical / sexual abuse, (ii) engaged in or apparently engaging in a sexual pose or activity, or (iii) in the presence of another person who is engaged in or apparently engaging in a sexual pose or activity; or</p> <p>b) the intimate image of a person who is or appears / implied to be below 16 years of age.</p>
Impersonation	Online activity conducted by a person (X) pretending to be the victim, without the victim's consent, and which is likely to cause a reasonable person to conclude that X is the victim.
Misuse of inauthentic material (e.g. deepfakes)	Online material which is a false audio and/or visual depiction of the victim or her likeness, communicated without the victim's consent, and which a reasonable person would conclude: <ul style="list-style-type: none"> - genuinely depicts the victim; and - is likely to cause the victim harassment, alarm, distress or humiliation.
Online statement instigating disproportionate harm ("OSIDH")	Online material that: <ul style="list-style-type: none"> - is published or intended to be published; - instigates or purports to instigate the public in Singapore or a section of the public in Singapore to act, or omit to act in a way to cause harm to the victim; and - is unjustifiable.
Hate speech	<p>Online communication to the public that incites or is likely to incite feelings of enmity, hatred, ill-will or hostility against, or contempt for or ridicule of a group or a member of the target group in Singapore by reason of that person's membership in the target group. The target group will be defined by a closed list of characteristics.</p> <p>Includes <u>violence-inciting content</u>: Online communication that urges another person, or a group of persons, to use force or violence against a group of persons ("target group"),¹⁹ or member of the target group in Singapore by reason of that person's membership in the target group, in Singapore.</p>

¹⁹ The target group can be defined by any characteristic.

Category of harm	Description
Misuse of personal information	<p>1) Communication of personal information that:</p> <ul style="list-style-type: none"> a) falls within a closed list; and b) was not available to the public at large prior to communication by the communicator; <p>2) A reasonable person would conclude that the communication is likely to cause the complainant harassment, alarm, distress or humiliation; and</p> <p>3) The complainant did not consent to the communication of the information.</p> <p>The “closed list” referred to in (1)(a) above comprises: (i) Physical, mental and medical conditions or state of health, and (ii) Personal financial and tax-related information.</p> <p><i>Note:</i> This will not cover any communication of information that is communicated pursuant to any written law, lawful duty or lawful power, or as required by law</p>
False statements	Published online material that contains or consists of a false statement of fact that is likely to cause harm to the subject of the false statement of fact
Statement affecting reputation (“SAR”)	Published online material that contains or consists of a statement (whether fact or opinion) that is likely to cause a reasonable person to have a lower estimation of the subject of the statement and which is likely to cause harm to the subject of the statement.

Annex D: Parties against whom directions may be issued

Communicator	A “communicator” of an online material is a person who posted the relevant material, and includes any other person who reposts identical copies of the relevant material posted.
Administrator	<p>An “administrator” of an online location is a person who:</p> <ul style="list-style-type: none">(a) develops and maintains the online location;(b) organises, manages or supervises the use of the online location;(c) manages or regulates membership of, or access to, the online location; or(d) has the authority to decide whether any material may be included or excluded on the online location, or where to place the material on the online location or otherwise exercise editorial control over the online location. <p>An “administrator” does not include a platform. To illustrate using a given social media page, the person who develops and maintains this page is its administrator, while the social media service is the platform.</p>
Platform	A “platform” is a person who provides the service by means of which the relevant material had been communicated through the internet. Examples of “platform” include but are not limited to social networking sites, search engines, dating applications, online games, email service providers and video publishing sites.

Annex E: Directions which the Agency may make

Categories of harm	Directions available against:		
	Communicator (“C”)	Administrator (“A”)	Platform (“P”)
All harms except False statements and SAR	<ul style="list-style-type: none"> - <u>Disable access to material</u>, which can extend to a category or class of content. - <u>Labelling</u>, which will require C to communicate in the specified manner in Singapore to any end user who accesses a specified online location, a notice setting out specified instances for which C has been subject to the Agency’s directions. 	<ul style="list-style-type: none"> - <u>Disable access to material by users in Singapore</u>, which can extend to a category or class of content. - <u>Remove</u> C’s account from the online group, and prevent that account from rejoining for up to 2 years. - <u>Closure of</u> the online group or location which A administers. - <u>Labelling</u>, which will require A to communicate in the specified manner in Singapore to any end user who accesses the online location which A administers, a notice setting out specified instances for which that online location has been subject to the Agency’s directions. 	<ul style="list-style-type: none"> - <u>Disable access to material by users in Singapore</u>, which can extend to a category or class of content for prescribed P. - <u>Deactivate</u> any or all of C’s account on P’s service, for a period of up to 2 years. - <u>Closure of</u> the online group or location complained of. - <u>Engagement reduction</u>²⁰, which will require a prescribed P to exercise control over engagement with content in order to protect victims. <p>Orders against P can include action to be taken against identical copies. This will be operationalised later for prescribed P.</p>
OSIDH, False statements and SAR	<ul style="list-style-type: none"> - <u>Right of Reply</u>²¹ which will require C to communicate a reply notice in a specified form and manner, to a specified person or description of persons. 	<ul style="list-style-type: none"> - <u>Right of Reply</u>, which will require A to communicate a reply notice in a specified form and manner, to a specified person or description of persons. 	<ul style="list-style-type: none"> - <u>Right of Reply</u>, which will require P to communicate by means of its service, a reply notice in a specified form and manner, to a specified person or description of persons.

²⁰ Engagement reduction directions will not be available in respect of the online harm of misuse of personal information.

²¹ The reply notice which C, A or P may be required to communicate will originate from the victim, and may be in the form of (a) the victim’s correction or rebuttal of the original statement, (b) the victim’s clarification or contextualisation of the original statement, or (c) the victim’s apology or expression of remorse.

Categories of harm	Directions available against:		
	Communicator ("C")	Administrator ("A")	Platform ("P")
	The Agency can also require (a) C to communicate the reply notice if C makes further communications which are identical or similar to the specified material, and (b) specified measures to ensure the reply notice has equal prominence to the specified material.	The Agency can also require specified measures to ensure the reply notice has equal prominence to the specified material	The Agency can also require specified measures to ensure the reply notice has equal prominence to the specified material

Annex F: Duties owed by parties under the statutory torts

1. The statutory torts will specify the obligations of communicators, administrators and platforms.
2. Duty of communicators: A person must not communicate and/or publish any specified online harm in Singapore through the internet, with the intention, knowledge or reasonable grounds to believe that doing so would cause loss or harm to the victim.
3. For instance, a communicator who publishes the identity information of another person online with the intent to cause harassment, alarm or distress to such person will be found in breach of this duty.
4. A communicator who breaches this duty will be liable for the loss or harm suffered by the victim, subject to a defence of reasonable conduct.
5. Furthermore, if the victim gave the communicator notice of the online harm, and the communicator failed to take steps to address that harm within 24 hours, the communicator may be liable for enhanced damages.
6. Duties of administrators: Administrators will have two duties:
 - a. **Duty 1**: An administrator must not create, set up or administer an online location in a manner that:
 - i. Encourages specified online harms at the online location, or
 - ii. Creates, enables or perpetuates a state of affairs that increases the risk of specified online harms at the online location,with the intention, knowledge or reason to believe that online harms would be likely to occur.

For instance, an administrator who sets up a chat group on a chat messaging application for members to trade intimate images of women without their consent will be found in breach of Duty 1.

Under this duty, and similar to communicators, administrators will be (i) able to rely on a defence of reasonable conduct, and (ii) liable for enhanced damages for failing to take steps within 24 hours to address a harm which is notified to them.
 - b. **Duty 2**: Administrators must act reasonably to address specified online harms at their online location *which they have been notified of*. This means carefully assessing the relevant circumstances, and considering whether and how the online harm should be addressed, including by:

- i. Disabling access to online harm; and
- ii. Preventing the further occurrence of the online harm.

For this duty, administrators may rely on a defence of reasonable excuse. The following factors will be relevant in assessing whether the defence is made out:

- i. Whether the administrator reasonably assessed that no specified online harms took place, or that it would be reasonable or appropriate not to take steps or measures in respect of the online harm; and
- ii. Whether it was reasonably practicable for the administrator to do more than what he in fact did to satisfy that duty.

7. These two duties are distinct. Administrators who have complied with Duty 1, can breach and be liable for a breach of Duty 2.
8. Duty of platforms: A platform must act reasonably to address specified online harms *which it has been given notice of*. This means carefully assessing the relevant circumstances, considering whether and how the online harm should be addressed, including by:
 - a. Disabling access to the online harm; and
 - b. Preventing the further occurrence of the online harm.
9. For prescribed platforms, it will be presumed that measures taken after a specified time-period (e.g. more than 24 hours after receipt of notice) would not be taken within a reasonable time. This will encourage timely action. However, it will be open to prescribed platforms to prove that more time was needed because the case was complex.
10. A platform's duty is only *triggered upon notice* – platforms will not need to pre-emptively monitor their services to avoid liability. Instead, a platform must assess notices from the victim, which must contain enough information about the online harm. If there is insufficient information in the notice, platforms will not be liable. For clarity, the information which must be in the notice may be prescribed.
11. Whether a platform has acted reasonably depends on all the circumstances. However, we recognise that platforms may receive large numbers of complaints. Therefore, we are considering specifying steps which, if performed by the platform, would go towards satisfying their duty under the statutory torts.

12. Platforms may rely on a *defence of reasonable excuse*. The following factors will be relevant in assessing whether the defence is made out:
 - a. Whether the platform reasonably assessed that no specified online harms took place, or that it would be reasonable or appropriate not to take steps or measures in respect of the online harm;
 - b. Whether it was reasonably practicable for the platform to do more than what it in fact did to satisfy that duty.

Remedies available under the statutory torts

13. If a Court finds that a party has breached their duty under the statutory torts, the party may be liable for damages. Further, the Court can grant injunctions to put a stop to the harm or to prevent further harm. This is consistent with existing practices for court claims under general tort law.
14. We also propose to specifically legislate that:
 - a. Damages for pure economic losses and an account of profits will be recoverable for specified online harms.
 - b. Minimum and maximum damages can be prescribed for specified online harms and/or categories of respondents.