

Legal questionnaire completed by Trilegal • April 2024

This document contains responses from the law firm listed above to a questionnaire distributed by NCMEC (questions are in **bold text**). Responses to the questionnaire may be limited to officially enacted legislation; it is possible that actual practice or enforcement of the law varies, and relevant court rulings or case law may also differ from legislative text. Responses have been reformatted and may have been slightly edited for clarity. Furthermore, responses may include commentary, paraphrasing, and unofficial translations of source material (e.g., national legislation) originally produced in other languages. Only official source documents in official languages should be relied upon as legally binding. This document serves to inform further research and does not constitute legal advice from NCMEC or the listed law firm.

1. What laws and regulations contain legal definitions of the following terms or corresponding terms in your local jurisdiction (links to existing U.S. legal definitions are included, where relevant, as background for comparison – please include definitions of any corresponding terms in your country):

a. child or minor (18 U.S.C. 2256(1), <https://www.law.cornell.edu/uscode/text/18/2256>)

1. Explanation to Section 67B (Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc., in Electronic Form) of the Information Technology Act, 2000, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077§ionId=13094§ionno=67B&orderno=85

'Children' means persons who has not completed the age of 18 years.

2. Section 2(1)(d) (Definitions) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686§ionId=12851§ionno=2&orderno=2

'Child' means any person below the age of eighteen years.

3. Section 2(12) (Definitions) of the Juvenile Justice (Care and Protection of Children) Act, 2015, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_000010_201602_1517807328168§ionId=12722§ionno=2&orderno=2

'Child' means a person who has not completed eighteen years of age.

4. Section 2(aa) (Definitions) of the Immoral Traffic (Prevention) Act, 1956, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_0_00015_1956104_1673601098535§ionId=72577§ionno=2&orderno=2

'Child' means a person who has not completed the age of sixteen years.

5. Section 2(cb) (Definitions) of the Immoral Traffic (Prevention) Act, 1956, available at <https://www.indiacode.nic.in/show->



[data?actid=AC_CEN_13_0_00015_1956104_1673601098535§ionId=72577§ionno=2&orderno=2](https://www.indiacode.nic.in/bitstream/123456789/1848/1/A1986-61.pdf)

'Minor' means a person who has completed the age of sixteen years but has not completed the age of eighteen years.

6. Section 2(f) (Definitions) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>

'Child' means an individual who has not completed the age of eighteen years.

7. Section 2(1)(d) (Definitions) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

'Child' means any person below the age of eighteen years.

8. Section 2(ii) (Definitions) of the Child and Adolescent Labour (Prohibition and Regulation) Act, 1986, available at <https://www.indiacode.nic.in/bitstream/123456789/1848/1/A1986-61.pdf>

'Child' means a person who has not completed his fourteenth year of age or such age as may be specified in the Right of Children to Free and Compulsory Education Act, 2009 (35 of 2009), whichever is more.

9. Section 2(a) (Definitions) of the Prohibition of Child Marriage Act, 2006, available at <https://www.indiacode.nic.in/bitstream/123456789/2055/1/A2007-06.pdf>

'Child' means a person who, if a male, has not completed twenty-one years of age, and if a female, has not completed eighteen years of age.

10. Section 2(f) (Definitions) of the Prohibition of Child Marriage Act, 2006, available at <https://www.indiacode.nic.in/bitstream/123456789/2055/1/A2007-06.pdf>

'Minor' means a person who, under the provisions of the Majority Act, 1875 (9 of 1875) is to be deemed not to have attained his majority.

- b. child sexual exploitation (Missing Children's Assistance Act of 2023, Section 2, (a)(1)(9), <https://www.congress.gov/118/bills/s2051/BILLS-118s2051es.pdf>)**

1. Explanation 1 to Section 141 (Trafficking of Person) of the BNS, available at https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nyaya_Sanhita_2023.pdf

The expression 'exploitation' shall include any act of physical exploitation or any form of sexual exploitation, slavery or practices similar to slavery, servitude, beggary or forced removal of organs.



2. Section 74 (Sexual Harassment and Punishment for Sexual Harassment) of the BNS, available at https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nyaya_Sanhita,_2023.pdf

- (1) A man committing any of the following acts -
- (i) physical contact and advances involving unwelcome and explicit sexual overtures; or
 - (ii) a demand or request for sexual favours; or
 - (iii) showing pornography against the will of a woman; or
 - (iv) making sexually coloured remarks,
- shall be guilty of the offence of sexual harassment.

3. Section 11 (Sexual Harassment) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686§ionId=12860§ionno=11&orderno=11

A person is said to commit sexual harassment upon a child when such person with sexual intent, -

- (i) utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or
- (ii) makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or
- (iii) shows any object to a child in any form or media for pornographic purposes; or
- (iv) repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means; or
- (v) threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or
- (vi) entices a child for pornographic purposes or gives gratification therefore.

Explanation - Any question which involves 'sexual intent' shall be a question of fact.

4. Section 5 (Procuring, Inducing or Taking Person for the Sake of Prostitution) of the Immoral Traffic (Prevention) Act, 1956, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_0_00015_1956104_1673601098535§ionId=72577§ionno=2&orderno=2

- (1) Any person who -
- (a) procures or attempts to procure a person, whether with or without his consent, for the purpose of prostitution; or
 - (b) induces a person to go from any place, with the intent that he may for the purpose of prostitution become the inmate of, or frequent, a brothel; or
 - (c) takes or attempts to take a person, or causes a person to be taken, from one place to another with a view to his carrying on, or being brought up to carry on prostitution; or
 - (d) causes or induces a person to carry on prostitution;



shall be punishable on conviction with rigorous imprisonment for a term of not less than three years and not more than seven years and also with fine which may extend to two thousand rupees, and if any offence under this sub-Section is committed against the will of any person, the punishment of imprisonment for a term of seven years shall extend to imprisonment for a term of fourteen years:

Provided that if the person in respect of whom an offence committed under this sub-Section -

- (i) is a child, the punishment provided under this sub-Section shall extend to rigorous imprisonment for a term of not less than seven years but may extend to life; and
 - (ii) is a minor, the punishment provided under this sub-Section shall extend to rigorous imprisonment for a term of not less than seven years and not more than fourteen years;
- (3) An offence under this Section shall be triable-
- (a) in the place from which a person is procured, induced to go, taken or caused to be taken or from which an attempt to procure or take such person is made; or
 - (b) in the place to which he may have gone as a result of the inducement or to which he is taken or caused to be taken or an attempt to take him is made.

**c. sexually explicit conduct (18 U.S.C. 2256(2),
<https://www.law.cornell.edu/uscode/text/18/2256>)**

Section 11 (Sexual Harassment) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686§ionId=12860§ionno=11&orderno=11

A person is said to commit sexual harassment upon a child when such person with sexual intent, -

- (i) utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or
- (ii) makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or
- (iii) shows any object to a child in any form or media for pornographic purposes; or
- (iv) repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means; or
- (v) threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or
- (vi) entices a child for pornographic purposes or gives gratification therefore.

Explanation - Any question which involves 'sexual intent' shall be a question of fact.

Section 67B (Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc., in Electronic Form) of the Information Technology Act, 2000,



available at <https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf>

Whoever, –

- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
- (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
- (d) facilitates abusing children online, or
- (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –
 - (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or
 - (ii) which is kept or used for bona fide heritage or religious purposes.

Explanation – For the purposes of this section, children means persons who has not completed the age of 18 years.

d. child sexual abuse (18 U.S.C. 2243(a), <https://www.law.cornell.edu/uscode/text/18/2243>)

1. Section 11 (Sexual Harassment) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686§ionId=12860§ionno=11&orderno=11

A person is said to commit sexual harassment upon a child when such person with sexual intent, –

- (i) utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or
- (ii) makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or
- (iii) shows any object to a child in any form or media for pornographic purposes; or
- (iv) repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means; or



- (v) threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or
- (vi) entices a child for pornographic purposes or gives gratification therefore.

Explanation - Any question which involves 'sexual intent' shall be a question of fact.

2. Section 3 (Penetrative Sexual Assault) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686&orderno=3

A person is said to commit 'penetrative sexual assault' if -

- (a) he penetrates his penis, to any extent, into the vagina, mouth, urethra or anus of a child or makes the child to do so with him or any other person; or
 - (b) he inserts, to any extent, any object or a part of the body, not being the penis, into the vagina, the urethra or anus of the child or makes the child to do so with him or any other person; or
 - (c) he manipulates any part of the body of the child so as to cause penetration into the vagina, urethra, anus or any part of body of the child or makes the child to do so with him or any other person; or
 - (d) he applies his mouth to the penis, vagina, anus, urethra of the child or makes the child to do so to such person or any other person.
3. Section 5 (Aggravated Penetrative Sexual Assault) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686&orderno=5
 - (a) Whoever, being a police officer, commits penetrative sexual assault on a child -
 - (i) within the limits of the police station or premises at which he is appointed; or
 - (ii) in the premises of any station house, whether or not situated in the police station, to which he is appointed; or
 - (iii) in the course of his duties or otherwise; or
 - (iv) where he is known as, or identified as, a police officer; or
 - (b) whoever being a member of the armed forces or security forces commits penetrative sexual assault on a child -
 - (i) within the limits of the area to which the person is deployed; or
 - (ii) in any areas under the command of the forces or armed forces; or
 - (iii) in the course of his duties or otherwise; or
 - (iv) where the said person is known or identified as a member of the security or armed forces; or
 - (c) whoever being a public servant commits penetrative sexual assault on a child; or
 - (d) whoever being on the management or on the staff of a jail, remand home, protection home, observation home, or other place of custody or care and protection established by or under any law for the time being in force, commits penetrative sexual assault on a child, being inmate of such jail, remand home, protection home, observation home, or other place of custody or care and protection; or



- (e) whoever being on the management or staff of a hospital, whether Government or private, commits penetrative sexual assault on a child in that hospital; or
- (f) whoever being on the management or staff of an educational institution or religious institution, commits penetrative sexual assault on a child in that institution; or
- (g) whoever commits gang penetrative sexual assault on a child.
Explanation - When a child is subjected to sexual assault by one or more persons of a group in furtherance of their common intention, each of such persons shall be deemed to have committed gang penetrative sexual assault within the meaning of this clause and each of such person shall be liable for that act in the same manner as if it were done by him alone; or
- (h) whoever commits penetrative sexual assault on a child using deadly weapons, fire, heated substance or corrosive substance; or
- (i) whoever commits penetrative sexual assault causing grievous hurt or causing bodily harm and injury or injury to the sexual organs of the child; or
- (j) whoever commits penetrative sexual assault on a child, which -
 - (i) physically incapacitates the child or causes the child to become mentally ill as defined under clause (b) of section 2 of the Mental Health Act, 1987(14 of 1987) or causes impairment of any kind so as to render the child unable to perform regular tasks, temporarily or permanently;
 - (ii) in the case of female child, makes the child pregnant as a consequence of sexual assault;
 - (iii) inflicts the child with Human Immunodeficiency Virus or any other life threatening disease or infection which may either temporarily or permanently impair the child by rendering him physically incapacitated, or mentally ill to perform regular tasks;
 - (iv) causes death of the child; or
- (k) whoever, taking advantage of a child's mental or physical disability, commits penetrative sexual assault on the child; or
- (l) whoever commits penetrative sexual assault on the child more than once or repeatedly; or
- (m) whoever commits penetrative sexual assault on a child below twelve years; or
- (n) whoever being a relative of the child through blood or adoption or marriage or guardianship or in foster care or having a domestic relationship with a parent of the child or who is living in the same or shared household with the child, commits penetrative sexual assault on such child; or
- (o) whoever being, in the ownership, or management, or staff, of any institution providing services to the child, commits penetrative sexual assault on the child; or



- (p) whoever being in a position of trust or authority of a child commits penetrative sexual assault on the child in an institution or home of the child or anywhere else; or
 - (q) whoever commits penetrative sexual assault on a child knowing the child is pregnant; or
 - (r) whoever commits penetrative sexual assault on a child and attempts to murder the child; or
 - (s) whoever commits penetrative sexual assault on a child in the course of communal or sectarian violence or during any natural calamity or in similar situations; or
 - (t) whoever commits penetrative sexual assault on a child and who has been previously convicted of having committed any offence under this Act or any sexual offence punishable under any other law for the time being in force; or
 - (u) whoever commits penetrative sexual assault on a child and makes the child to strip or parade naked in public, is said to commit aggravated penetrative sexual assault.
4. Section 7 (Sexual Assault) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686&orderno=7

Whoever, with sexual intent touches the vagina, penis, anus or breast of the child or makes the child touch the vagina, penis, anus or breast of such person or any other person, or does any other act with sexual intent which involves physical contact without penetration is said to commit sexual assault.

5. Section 9 (Aggravated Sexual Assault) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686&orderno=9
- (a) Whoever, being a police officer, commits sexual assault on a child -
 - (i) within the limits of the police station or premises where he is appointed; or
 - (ii) in the premises of any station house whether or not situated in the police station to which he is appointed; or
 - (iii) in the course of his duties or otherwise; or
 - (iv) where he is known as, or identified as a police officer; or
 - (b) whoever, being a member of the armed forces or security forces, commits sexual assault on a child -
 - (i) within the limits of the area to which the person is deployed; or
 - (ii) in any areas under the command of the security or armed forces; or
 - (iii) in the course of his duties or otherwise; or
 - (iv) where he is known or identified as a member of the security or armed forces; oror
 - (c) whoever being a public servant commits sexual assault on a child; or



- (d) whoever being on the management or on the staff of a jail, or remand home or protection home or observation home, or other place of custody or care and protection established by or under any law for the time being in force commits sexual assault on a child being inmate of such jail or remand home or protection home or observation home or other place of custody or care and protection; or
- (e) whoever being on the management or staff of a hospital, whether Government or private, commits sexual assault on a child in that hospital; or
- (f) whoever being on the management or staff of an educational institution or religious institution, commits sexual assault on a child in that institution; or
- (g) whoever commits gang sexual assault on a child.
Explanation. - when a child is subjected to sexual assault by one or more persons of a group in furtherance of their common intention, each of such persons shall be deemed to have committed gang sexual assault within the meaning of this clause and each of such person shall be liable for that act in the same manner as if it were done by him alone; or
- (h) whoever commits sexual assault on a child using deadly weapons, fire, heated substance or corrosive substance; or
- (i) whoever commits sexual assault causing grievous hurt or causing bodily harm and injury or injury to the sexual organs of the child; or
- (j) whoever commits sexual assault on a child, which -
 - (i) physically incapacitates the child or causes the child to become mentally ill as defined under clause (l) of section 2 of the Mental Health Act, 1987(14 of 1987) or causes impairment of any kind so as to render the child unable to perform regular tasks, temporarily or permanently; or
 - (ii) inflicts the child with Human Immunodeficiency Virus or any other life threatening disease or infection which may either temporarily or permanently impair the child by rendering him physically incapacitated, or mentally ill to perform regular tasks; or
- (k) whoever, taking advantage of a child's mental or physical disability, commits sexual assault on the child; or
- (l) whoever commits sexual assault on the child more than once or repeatedly; or
- (m) whoever commits sexual assault on a child below twelve years; or
- (n) whoever, being a relative of the child through blood or adoption or marriage or guardianship or in foster care, or having domestic relationship with a parent of the child, or who is living in the same or shared household with the child, commits sexual assault on such child; or



- (o) whoever, being in the ownership or management or staff, of any institution providing services to the child, commits sexual assault on the child in such institution; or
 - (p) whoever, being in a position of trust or authority of a child, commits sexual assault on the child in an institution or home of the child or anywhere else; or
 - (q) whoever commits sexual assault on a child knowing the child is pregnant; or
 - (r) whoever commits sexual assault on a child and attempts to murder the child; or
 - (s) whoever commits sexual assault on a child in the course of communal or sectarian violence or during any natural calamity or in any similar situations; or
 - (t) whoever commits sexual assault on a child and who has been previously convicted of having committed any offence under this Act or any sexual offence punishable under any other law for the time being in force; or
 - (u) whoever commits sexual assault on a child and makes the child to strip or parade naked in public, is said to commit aggravated sexual assault.
 - (v) whoever persuades, induces, entices or coerces a child to get administered or administers or direct anyone to administer, help in getting administered any drug or hormone or any chemical substance, to a child with the intent that such child attains early sexual maturity.
6. Section 74(1) (Sexual Harassment and Punishment for Sexual Harassment) of the BNS, available at https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nyaya_Sanhita,_2023.pdf
- A man committing any of the following acts—
- (i) physical contact and advances involving unwelcome and explicit sexual overtures; or
 - (ii) a demand or request for sexual favours; or
 - (iii) showing pornography against the will of a woman; or
 - (iv) making sexually coloured remarks,
- shall be guilty of the offence of sexual harassment.
7. Section 67B (Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc., in Electronic Form) of the Information Technology Act, 2000, available at <https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf>
- Whoever, –
- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or



- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
- (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
- (d) facilitates abusing children online, or
- (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –

- (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or
- (ii) which is kept or used for bona fide heritage or religious purposes.

Explanation – For the purposes of this section, children means persons who has not completed the age of 18 years.

8. Section 5 (Procuring, Inducing or Taking Person for the Sake of Prostitution) of the Immoral Traffic (Prevention) Act, 1956, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_0_00015_1956104_1673601098535§ionId=72577§ionno=2&orderno=2

(1) Any person who -

- (a) procures or attempts to procure a person, whether with or without his consent, for the purpose of prostitution; or
- (b) induces a person to go from any place, with the intent that he may for the purpose of prostitution become the inmate of, or frequent, a brothel; or
- (c) takes or attempts to take a person, or causes a person to be taken, from one place to another with a view to his carrying on, or being brought up to carry on prostitution; or
- (d) causes or induces a person to carry on prostitution;

shall be punishable on conviction with rigorous imprisonment for a term of not less than three years and not more than seven years and also with fine which may extend to two thousand rupees, and if any offence under this sub-Section is committed against the will of any person, the punishment of imprisonment for a term of seven years shall extend to imprisonment for a term of fourteen years:

Provided that if the person in respect of whom an offence committed under this sub-Section -



- (i) is a child, the punishment provided under this sub-Section shall extend to rigorous imprisonment for a term of not less than seven years but may extend to life; and
- (ii) is a minor, the punishment provided under this sub-Section shall extend to rigorous imprisonment for a term of not less than seven years and not more than fourteen years;

(3) An offence under this Section shall be triable-

- (a) in the place from which a person is procured, induced to go, taken or caused to be taken or from which an attempt to procure or take such person is made; or
- (b) in the place to which he may have gone as a result of the inducement or to which he is taken or caused to be taken or an attempt to take him is made.

9. Section 67 (Punishment for Publishing or Transmitting Obscene Material in Electronic Form) of the Information Technology Act, 2000, available at https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

10. Section 67A (Punishment for Publishing or Transmitting of Material Containing Sexually Explicit Act, etc., in Electronic Form) of the Information Technology Act, 2000, available at https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

- e. **child pornography or child sexual abuse material (CSAM) (18 U.S.C. 2256(8)),** <https://www.law.cornell.edu/uscode/text/18/2256>

1. Section 2(da) (Definitions) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686&orderno=2

'Child pornography' means any visual depiction of sexually explicit conduct involving a child which include photograph, video, digital or computer generated image indistinguishable from an actual child and image created, adapted, or modified, but appear to depict a child.



2. Section 67B (Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc., in Electronic Form) of the Information Technology Act, 2000, available at <https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf>

Whoever, –

- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
- (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
- (d) facilitates abusing children online, or
- (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –
 - (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or
 - (ii) which is kept or used for bona fide heritage or religious purposes.

Explanation – For the purposes of this section, children means persons who has not completed the age of 18 years.

- f. **computer-generated images or videos of child pornography or CSAM (created by artificial intelligence or morphed) (18 U.S.C. 2256(8) & (9),** <https://www.law.cornell.edu/uscode/text/18/2256>)

Section 67B (Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc., in Electronic Form) of the Information Technology Act, 2000, available at <https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf>

Whoever, –

- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children



- in obscene or indecent or sexually explicit manner; or
- (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
- (d) facilitates abusing children online, or
- (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form-
 - (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or
 - (ii) which is kept or used for bonafide heritage or religious purposes.

Explanation - For the purposes of this section 'children' means persons who has not completed the age of 18 years.

g. enticement or grooming (encouraging, persuading, or coercing a child to engage in sexual activity or to create child pornography or CSAM) (18 U.S.C. 2422(b), <https://www.law.cornell.edu/uscode/text/18/2422>)

1. Section 11 (Sexual Harassment) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686§ionId=12860§ionno=11&orderno=11

A person is said to commit sexual harassment upon a child when such person with sexual intent, -

- (i) utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or
- (ii) makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or
- (iii) shows any object to a child in any form or media for pornographic purposes; or
- (iv) repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means; or
- (v) threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or
- (vi) entices a child for pornographic purposes or gives gratification therefore.

Explanation - Any question which involves 'sexual intent' shall be a question of fact.



2. Section 141(1) (Trafficking of Persons) of the BNS, available at https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nyaya_Sanhita,_2023.pdf

Whoever, for the purpose of exploitation, recruits, transports, harbours, transfers, or receives, a person or persons, by -

- (a) using threats; or
- (b) using force, or any other form of coercion; or
- (c) by abduction; or
- (d) by practicing fraud, or deception; or
- (e) by abuse of power; or
- (f) by inducement, including the giving or receiving of payments or benefits, in order to achieve the consent of any person having control over the person recruited, transported, harboured, transferred or received,

commits the offence of trafficking.

Explanation 1 — The expression “exploitation” shall include any act of physical exploitation or any form of sexual exploitation, slavery or practices similar to slavery, servitude, beggary or forced removal of organs.

Explanation 2 — The consent of the victim is immaterial in determination of the offence of trafficking.

3. Section 67B (Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc., in Electronic Form) of the Information Technology Act, 2000, available at <https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf>

Whoever, –

- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
- (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
- (d) facilitates abusing children online, or
- (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:



Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –

- (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or
- (ii) which is kept or used for bona fide heritage or religious purposes.

Explanation – For the purposes of this section, children means persons who has not completed the age of 18 years.

4. Section 5 (Procuring, Inducing or Taking Person for the Sake of Prostitution) of the Immoral Traffic (Prevention) Act, 1956, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_0_00015_1956104_1673601098535§ionId=72577§ionno=2&orderno=2

(1) Any person who -

- (a) procures or attempts to procure a person, whether with or without his consent, for the purpose of prostitution; or
- (b) induces a person to go from any place, with the intent that he may for the purpose of prostitution become the inmate of, or frequent, a brothel; or
- (c) takes or attempts to take a person, or causes a person to be taken, from one place to another with a view to his carrying on, or being brought up to carry on prostitution; or
- (d) causes or induces a person to carry on prostitution;

shall be punishable on conviction with rigorous imprisonment for a term of not less than three years and not more than seven years and also with fine which may extend to two thousand rupees, and if any offence under this sub-Section is committed against the will of any person, the punishment of imprisonment for a term of seven years shall extend to imprisonment for a term of fourteen years:

Provided that if the person in respect of whom an offence committed under this sub-Section -

- (i) is a child, the punishment provided under this sub-Section shall extend to rigorous imprisonment for a term of not less than seven years but may extend to life; and
- (ii) is a minor, the punishment provided under this sub-Section shall extend to rigorous imprisonment for a term of not less than seven years and not more than fourteen years;

(3) An offence under this Section shall be triable-

- (a) in the place from which a person is procured, induced to go, taken or caused to be taken or from which an attempt to procure or take such person is made; or
- (b) in the place to which he may have gone as a result of the inducement or to which he is taken or caused to be taken or an attempt to take him is made.



5. Section 6(3) (Detaining a Person in Premises where Prostitution is Carried On) of the Immoral Traffic (Prevention) Act, 1956, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_0_00015_1956104_1673601098535§ionId=72577§ionno=2&orderno=2

A person shall be presumed to detain a woman or girl in a brothel or in or upon any premises for the purpose of sexual intercourse with a man other than her lawful husband, if such person, with intent to compel or induce her to remain there,-

- (a) withholds from her any jewellery, wearing apparel, money or other property belonging to her, or
 - (b) threatens her with legal proceedings if she takes away with her any jewellery, wearing apparel, money or other property lent or supplied to her by or by the direction of such person.
6. Section 67 (Punishment for Publishing or Transmitting Obscene Material in Electronic Form) of the Information Technology Act, 2000, available at https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

7. Section 67A (Punishment for Publishing or Transmitting of Material Containing Sexually Explicit Act, etc., in Electronic Form) of the Information Technology Act, 2000, available at https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

h. legal age of consent for sexual activity – are there laws and regulations, if so, what ages are specified?

1. Section 11 (Who are Competent to Contract) of the Indian Contract Act, 1872, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_3_20_00035_187209_1523268996428&orderno=11

Every person is competent to contract who is of the age of majority according to the law to which he is subject, and who is of sound mind and is not disqualified from contracting by any law to which he is subject.



2. Section 3(1) (Definitions) of the Majority Act, 1875, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_3_20_00038_187509_1523269774430§ionId=44325§ionno=3&orderno=3

Every person domiciled in India shall attain the age of majority on his completing the age of eighteen years and not before.

3. As per the Protection of Children from Sexual Offences Act, 2012, any sexual act committed by a person with a minor (i.e., a person below the age of eighteen years) is an offence.
- i. **Sextortion (extorting money or sexual favors from a child by threatening to share sexually explicit, child pornography or CSAM images of the child) (Missing Children's Assistance Act of 2023, Section 2, (a)(1)(8), <https://www.congress.gov/118/bills/s2051/BILLS-118s2051es.pdf>)**

1. Section 11 (Sexual Harassment) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686§ionId=12860§ionno=11&orderno=11

A person is said to commit sexual harassment upon a child when such person with sexual intent, -

- (i) utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or
- (ii) makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or
- (iii) shows any object to a child in any form or media for pornographic purposes; or
- (iv) repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means; or
- (v) threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or
- (vi) entices a child for pornographic purposes or gives gratification therefore.

Explanation – Any question which involves 'sexual intent' shall be a question of fact.

2. Section 94 (Procuration of Child) of the BNS, available at https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nyaya_Sanhita_2023.pdf

Whoever, by any means whatsoever, induces any child below the age of eighteen years to go from any place or to do any act with intent that such child below the age of eighteen years may be, or knowing that it is likely that such child will be, forced or seduced to illicit intercourse with another person shall be punishable with imprisonment



which may extend to ten years, and shall also be liable to fine.

3. Section 5 (Procuring, Inducing or Taking Person for the Sake of Prostitution) of the Immoral Traffic (Prevention) Act, 1956, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_0_00015_1956104_1673601098535§ionId=72577§ionno=2&orderno=2

(1) Any person who -

- (a) procures or attempts to procure a person, whether with or without his consent, for the purpose of prostitution; or
- (b) induces a person to go from any place, with the intent that he may for the purpose of prostitution become the inmate of, or frequent, a brothel; or
- (c) takes or attempts to take a person, or causes a person to be taken, from one place to another with a view to his carrying on, or being brought up to carry on prostitution; or
- (d) causes or induces a person to carry on prostitution;

shall be punishable on conviction with rigorous imprisonment for a term of not less than three years and not more than seven years and also with fine which may extend to two thousand rupees, and if any offence under this sub-Section is committed against the will of any person, the punishment of imprisonment for a term of seven years shall extend to imprisonment for a term of fourteen years:

Provided that if the person in respect of whom an offence committed under this sub-Section -

- (i) is a child, the punishment provided under this sub-Section shall extend to rigorous imprisonment for a term of not less than seven years but may extend to life; and
- (ii) is a minor, the punishment provided under this sub-Section shall extend to rigorous imprisonment for a term of not less than seven years and not more than fourteen years;

(3) An offence under this Section shall be triable-

- (a) in the place from which a person is procured, induced to go, taken or caused to be taken or from which an attempt to procure or take such person is made; or
- (b) in the place to which he may have gone as a result of the inducement or to which he is taken or caused to be taken or an attempt to take him is made.

4. Section 6(3) (Detaining a Person in Premises where Prostitution is Carried On) of the Immoral Traffic (Prevention) Act, 1956, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_0_00015_1956104_1673601098535§ionId=72577§ionno=2&orderno=2

A person shall be presumed to detain a woman or girl in a brothel or in or upon any premises for the purpose of sexual intercourse with a man other than her lawful husband, if such person, with intent to compel or induce her to remain there,-

- (a) withholds from her any jewellery, wearing apparel, money or other property belonging to her, or
- (b) threatens her with legal proceedings if she takes away with her any jewellery, wearing apparel, money or other property lent or supplied to her by or by the

direction of such person.

2. Please explain any legal or regulatory requirement or recommendation for Online Platforms to undertake any of the following activities on their systems to protect children online from sexual exploitation:

a. review, screen, moderate, or detect content to identify child pornography or CSAM content

1. Rule 3(1)(b) (Due Diligence by an Intermediary) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The intermediary shall inform its rules and regulations, privacy policy and user agreement to the user in English or any language specified in the Eighth Schedule to the Constitution in the language of his choice and shall make reasonable efforts by itself, and to cause the users of its computer resource to not host, display, upload, modify, publish, transmit, store, update or share any information that, -

- (i) belongs to another person and to which the user does not have any right;
- (ii) is obscene, pornographic, paedophilic, invasive of another's privacy including bodily privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or an online game that causes user harm, or promoting enmity between different groups on the grounds of religion or caste with the intent to incite violence;
- (iii) is harmful to child;
- (iv) infringes any patent, trademark, copyright or other proprietary rights;
- (v) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature or, in respect of any business of the Central Government, is identified as fake or false or misleading by such fact check unit of the Central Government as the Ministry may, by notification published in the Official Gazette, specify;
- (vi) impersonates another person;
- (vii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting other nation;
- (viii) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
- (ix) is in the nature of an online game that is not verified as a permissible online game;
- (x) is in the nature of advertisement or surrogate advertisement or promotion of an online game that is not a permissible online game, or of any online gaming intermediary offering such an online game;
- (xi) violates any law for the time being in force.

Explanation - In this clause, "user harm" and "harm" mean any effect which is detrimental to a user or child, as the case may be.



[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

2. Rule 4(4) (Additional Due Diligence to be Observed by Significant Social Media Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:

Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:

Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this sub-rule, including a periodic review of any automated tools deployed by such intermediary:

Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.

[Trilegal Note: According to Section 2(1)(v) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, a significant social media intermediary means a social media intermediary (i.e., an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services) having fifty lakh registered users in India.]

b. review, screen, moderate, or detect content to identify enticement, grooming, or sextortion of a child

1. Rule 3(1)(b) (Due Diligence by an Intermediary) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732



[4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf](#)

The intermediary shall inform its rules and regulations, privacy policy and user agreement to the user in English or any language specified in the Eighth Schedule to the Constitution in the language of his choice and shall make reasonable efforts by itself, and to cause the users of its computer resource to not host, display, upload, modify, publish, transmit, store, update or share any information that, -

- (i) belongs to another person and to which the user does not have any right;
- (ii) is obscene, pornographic, paedophilic, invasive of another's privacy including bodily privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or an online game that causes user harm, or promoting enmity between different groups on the grounds of religion or caste with the intent to incite violence;
- (iii) is harmful to child;
- (iv) infringes any patent, trademark, copyright or other proprietary rights;
- (v) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature or, in respect of any business of the Central Government, is identified as fake or false or misleading by such fact check unit of the Central Government as the Ministry may, by notification published in the Official Gazette, specify;
- (vi) impersonates another person;
- (vii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting other nation;
- (viii) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
- (ix) is in the nature of an online game that is not verified as a permissible online game;
- (x) is in the nature of advertisement or surrogate advertisement or promotion of an online game that is not a permissible online game, or of any online gaming intermediary offering such an online game;
- (xi) violates any law for the time being in force.

Explanation - In this clause, "user harm" and "harm" mean any effect which is detrimental to a user or child, as the case may be.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

2. Rule 4(4) (Additional Due Diligence to be Observed by Significant Social Media Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf



A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:

Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:

Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this sub-rule, including a periodic review of any automated tools deployed by such intermediary:

Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.

[Trilegal Note: According to Section 2(1)(v) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, a significant social media intermediary means a social media intermediary (i.e., an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services) having fifty lakh registered users in India.]

c. report child pornography, CSAM, enticement, grooming, or sextortion that they become aware of or are notified about on their systems to a law enforcement or government agency or nongovernmental organization

1. Section 19(1) (Reporting of Offences) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686§ionId=12868§ionno=19&orderno=19

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any person (including the child), who has apprehension that in offence under this Act is likely to be committed or has knowledge that such an offence has been committed, he shall provide such information to, -

- (a) the Special Juvenile Police Unit; or
 - (b) the local police.
2. Rule 11 (Reporting of Pornographic Material Involving Child) of the Protection of Children from Sexual Offences Rules, 2020, available at



https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf

- (1) Any person who has received any pornographic material involving a child or any information regarding such pornographic material being stored, possessed, distributed, circulated, transmitted, facilitated, propagated or displayed, or is likely to be distributed, facilitated or transmitted in any manner shall report the contents to the SJPU or local police, or as the case may be, cyber-crime portal (cybercrime.gov.in) and upon such receipt of the report, the SJPU or local police or the cyber-crime portal take necessary action as per the directions of the Government issued from time to time.
- (2) In case the "person" as mentioned in sub-rule (1) is an "intermediary" as defined in clause (w) of sub-section (1) of section 2 of the Information Technology Act, 2000, such person shall in addition to reporting, as provided under sub-rule (1), also hand over the necessary material including the source from which such material may have originated to the SJPU or local police, or as the case may be, cyber-crime portal (cybercrime.gov.in) and upon such receipt of the said material, the SJPU or local police or the cyber-crime portal take necessary action as per the directions of the Government issued from time to time.
- (3) The report shall include the details of the device in which such pornographic content was noticed and the suspected device from which such content was received including the platform on which the content was displayed.

d. remove or take down any child pornography, CSAM, enticement, grooming, or sextortion that they identify, become aware of, or are notified about

1. Rule 3(1)(c) (Due Diligence by an Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

An intermediary shall periodically inform its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be.

[Trilegal Note: According to Rule 3(1)(b) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, an intermediary is required to undertake the following measures:

The rules and regulations, privacy policy or user agreement of the intermediary shall inform the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that, —

- (i) belongs to another person and to which the user does not have any right;
- (ii) is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;
- (iii) is harmful to child;



- (iv) infringes any patent, trademark, copyright or other proprietary rights;
- (v) violates any law for the time being in force;
- (vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;
- (vii) impersonates another person;
- (viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation;
- (ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
- (x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person.

Further, as per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

2. Rule 3(1)(d) (Due Diligence by an Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

An intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force:

Provided that any notification made by the Appropriate Government or its agency in relation to any information which is prohibited under any law for the time being in force shall be issued by an authorised agency, as may be notified by the Appropriate Government:

Provided further that if any such information is hosted, stored or published, the intermediary shall remove or disable access to that information, as early as possible, but in no case later than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency, as the case may be:

Provided also that the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under



clause (b) on a voluntary basis, or on the basis of grievances received under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a) or (b) of sub-section (2) of section 79 of the Act.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

3. Rule 3(2)(b) (Due Diligence by an Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

e. review content by human moderators to screen or moderate for child pornography or CSAM

1. Rule 4(4) (Additional Due Diligence to be Observed by Significant Social Media Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:



Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:

Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this sub-rule, including a periodic review of any automated tools deployed by such intermediary:

Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.

f. remove child pornography, CSAM, enticement, grooming, or sextortion from their systems when notified of its presence by a victim, nongovernmental organization, law enforcement, or government agency

1. Rule 3(1)(c) (Due Diligence by an Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

An intermediary shall periodically inform its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be.

[Trilegal Note: According to Rule 3(1)(b) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, an intermediary is required to undertake the following measures:

The rules and regulations, privacy policy or user agreement of the intermediary shall inform the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that, —

- (i) belongs to another person and to which the user does not have any right;
- (ii) is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;
- (iii) is harmful to child;
- (iv) infringes any patent, trademark, copyright or other proprietary rights;
- (v) violates any law for the time being in force;
- (vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;
- (vii) impersonates another person;



- (viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation;
- (ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
- (x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person.

Further, as per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

2. Rule 3(1)(d) (Due Diligence by an Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

An intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force:

Provided that any notification made by the Appropriate Government or its agency in relation to any information which is prohibited under any law for the time being in force shall be issued by an authorised agency, as may be notified by the Appropriate Government:

Provided further that if any such information is hosted, stored or published, the intermediary shall remove or disable access to that information, as early as possible, but in no case later than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency, as the case may be:

Provided also that the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under clause (b) on a voluntary basis, or on the basis of grievances received under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a) or (b) of sub-section (2) of section 79 of the Act.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply



to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

3. Rule 3(2)(b) (Due Diligence by an Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

- g. **use any specific technology to detect, remove, block, or take down any child pornography, CSAM, enticement, grooming, or sextortion, including:**
 - i. **“Hashing technology”** (<https://www.thorn.org/blog/hashing-detect-child-sex-abuse-imagery/>). Many Online Platforms hash and tag images and videos of child pornography or CSAM and then use hashing technology to scan content on their systems to detect the distribution of child pornography or CSAM online so it can be removed.
 - ii. **Artificial intelligence or machine learning tools to detect the presence of child pornography, CSAM, enticement, grooming, or sextortion.**

Indian laws do not require online platforms to use any specific technology to detect, remove, block, or take down any child pornography, CSAM, enticement, grooming, or sextortion.

- h. **if the applicable laws or regulations require some, but not all, Online Platforms to perform any of the above activities, describe how the differing requirements apply. For example, are differences based on the number of online users, types of services offered, etc.?**

Under the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, only a 'significant social media intermediary' is required to undertake the following activities on its systems to protect children online from sexual exploitation:

- (a) review, screen, moderate, or detect content to identify child pornography or CSAM content;
- (b) review, screen, moderate, or detect content to identify enticement, grooming, or sextortion of a child; and

- (c) review content by human moderators to screen or moderate for child pornography or CSAM.

Significant social media intermediary means a social media intermediary (i.e., an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services) having fifty lakh registered users in India.

3. Are Online Platforms legally required or recommended to implement any method to verify the age of a user before allowing access to an online platform?

1. Rule 4(12) (Additional Due Diligence to be Observed by Significant Social Media Intermediary and Online Gaming Intermediary) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

An online gaming intermediary shall, before accepting any deposit in cash or kind from any user for a permissible online real money game, identify such user and verify his identity:

Provided that the procedure required to be followed by an entity regulated by the Reserve Bank of India for identification and verification of a customer at the commencement of an account-based relationship shall apply, mutatis mutandis, in identification and verification of the users of such online gaming intermediary.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

2. Section 16 (Customer Due Diligence Procedure in case of Individuals) of the Master Direction - Know Your Customer (KYC) Directions, 2016, available at <https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/MD18KYCF6E92C82E1E1419D87323E3869BC9F13.pdf>

For undertaking Customer Due Diligence (CDD), Regulated Entities (REs) shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

- (a) the Aadhaar number where,
- (i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
 - (ii) he decides to submit his Aadhaar number voluntarily to a bank or any RE notified under first proviso to sub-section (1) of section 11A of the Prevention of Money Laundering Act, 2002; or
- (aa) the proof of possession of Aadhaar number where offline verification can be carried out; or



- (ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any officially valid documents (OVD) or the equivalent e-document thereof containing the details of his identity and address; or
- (ac) the KYC Identifier with an explicit consent to download records from Central Know Your Customer Registry (CKYCR); and
- (b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
- (c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the RE:

Provided that where the customer has submitted,

- i) Aadhaar number under clause (a) above to a bank or to a RE notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank or RE shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the RE.
- ii) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the RE shall carry out offline verification.
- iii) an equivalent e-document of any OVD, the RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I.
- iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the RE shall carry out verification through digital KYC as specified under Annex I.
- v) KYC Identifier under clause (ac) above, the RE shall retrieve the KYC records online from the CKYCR in accordance with Section 56.

Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the RE pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, REs shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the RE and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. REs shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the RE and shall be available for supervisory review.

Explanation 1: RE shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

3. Section 17 (Customer Due Diligence Procedure in case of Individuals) of the Master Direction - Know Your Customer (KYC) Directions, 2016, available at <https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/MD18KYCF6E92C82E1E1419D87323E3869BC9F13.pdf>

Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

- i. There must be a specific consent from the customer for authentication through OTP.
- ii. As a risk-mitigating measure for such accounts, REs shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. REs shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
- iii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (vi) below is complete.
- iv. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
- v. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
- vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
- vii. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
- viii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in nonface-to-face mode with any other RE. Further, while uploading KYC information to CKYCR, REs shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
- ix. REs shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

4. Section 18 (Customer Due Diligence Procedure in case of Individuals) of the Master Direction - Know Your Customer (KYC) Directions, 2016, available at <https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/MD18KYCF6E92C82E1E1419D87323E3869BC9F13.pdf>

REs may undertake video based customer identification process (V-CIP) to carry out:

- i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. Provided that in case of CDD of a proprietorship firm, REs shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28 and Section 29, apart from undertaking CDD of the proprietor.
- ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17.
- iii) Updation/Periodic updation of KYC for eligible customers.

REs opting to undertake V-CIP, shall adhere to the following minimum standards:

(a) V-CIP Infrastructure

- i) The RE should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the RE and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the RE only and all the data including video recording is transferred to the RE's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the RE.
- ii) The RE shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.
- iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
- iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.
- v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the RE. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.
- vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity

through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

- vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.
- viii) The V-CIP application software and relevant application programming interface (APIs) / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure

- i) Each RE shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the RE specially trained for this purpose. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.
- ii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the RE. However, in case of call drop / disconnection, fresh session shall be initiated.
- iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.
- iv) Any prompting observed at end of customer shall lead to rejection of the account opening process.
- v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work-flow.
- vi) The authorised official of the RE performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
 - a) OTP based Aadhaar e-KYC authentication
 - b) Offline Verification of Aadhaar for identification
 - c) KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer
 - d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLockerRE shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

In case of offline verification of Aadhaar using extensible markup language (XML) file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, REs shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, REs shall ensure that no incremental risk is added due to this.

- vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.
 - viii) RE shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through DigiLocker.
 - ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
 - x) The authorised official of the RE shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.
 - xi) Assisted V-CIP shall be permissible when banks take help of Business Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.
 - xii) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.
 - xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the RE.
- (c) V-CIP Records and Data Management
- i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. REs shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.
 - ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

5. Rule 4A(3) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The online gaming self-regulatory body, upon an application made to it by its member in respect of an online real money game, may declare such online real money game as a permissible online real money game, if, after making such inquiry as it deems fit, it is satisfied that -

- (a) the online real money game does not involve wagering on any outcome; and
- (b) the online gaming intermediary and such online game is in compliance with the provisions of rules 3 and 4, the provisions of any law relating to the age at which an individual is competent to enter into a contract, and the framework made by the online gaming self-regulatory body under sub-rule (8):

Provided that an online gaming self-regulatory body may, initially rely upon the information furnished by the applicant for verification of the online real money game and declare such game as a permissible online real money game for a period not exceeding three months:

Provided further that the online gaming self-regulatory body shall endeavour to complete the inquiry within the said period of three months and, upon its completion, either declare the online real money game as a permissible online real money game or inform the applicant in writing with the reasons thereof that such online game does not meet the requirements under these rules.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

6. Rule 4A(8) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The online gaming self-regulatory body shall prominently publish on its website, mobile based application or both, as the case may be, a framework for verifying an online real money game, which, among other things, includes the following, namely -

- (a) the measures to ensure that such online real money game is not against the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States and public order;
- (b) the safeguards against user harm, including self-harm and psychological harm;
- (c) the measures to safeguard children, including measures for parental or access control and classifying online games through age-rating mechanism, based on the nature and type of content; and
- (d) the measures to safeguard users against the risk of gaming addiction, financial loss and financial fraud, including repeated warning messages at higher frequency beyond a reasonable duration for a gaming session and provision to enable a user to exclude himself upon user-defined limits being reached for time or money spent.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government

notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

7. Under the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, only an online gaming intermediary (which enables its users to access online real money games) is required to implement methods to verify the age of a user before allowing access to the platform.

An online gaming intermediary means an intermediary that enables the users of its computer resource to access one or more online games.

An online real money game means an online game where a user makes a deposit in cash or kind with the expectation of earning winnings on that deposit.

Explanation - Winnings mean any prize, in cash or kind, which is distributed or intended to be distributed to a user of an online game based on the performance of the user and in accordance with the rules of such online game.

4. Are Online Platforms legally required or recommended to implement any method to obtain parental consent before a child uses the services of such Online Platforms?

1. Section 9 (Processing of Personal Data of Children) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf> -

- (1) The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed.

Explanation - For the purpose of this sub-section, the expression 'consent of the parent' includes the consent of lawful guardian, wherever applicable.

- (2) A Data Fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child.
- (3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.
- (4) The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed.
- (5) The Central Government may, if satisfied that a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (1) and (3) in respect of processing by that Data Fiduciary as the notification may specify.

Please note that:



- a) Section 2(i) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>, defines 'data fiduciary' as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
- b) Section 2(w) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>, defines 'Processing', in relation to personal data, to mean a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.
- c) Section 2(t) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>, defines 'Personal data' as any data about an individual who is identifiable by or in relation to such data.

[Trilegal Note: The Digital Personal Data Protection Act, 2023 (DPDPA) has been passed by both the houses of legislature and assented to by the President of India and is currently awaiting notification by the government in the official gazette. The aforementioned provision will come into effect once the DPDPA is notified.]

2. Rule 4A(8) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The online gaming self-regulatory body shall prominently publish on its website, mobile based application or both, as the case may be, a framework for verifying an online real money game, which, among other things, includes the following, namely -

- (a) the measures to ensure that such online real money game is not against the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States and public order;
- (b) the safeguards against user harm, including self-harm and psychological harm;
- (c) the measures to safeguard children, including measures for parental or access control and classifying online games through age-rating mechanism, based on the nature and type of content; and
- (d) the measures to safeguard users against the risk of gaming addiction, financial loss and financial fraud, including repeated warning messages at higher frequency beyond a reasonable duration for a gaming session and provision to enable a user to exclude himself upon user-defined limits being reached for time or money spent.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

3. A data fiduciary (defined above) and an online gaming intermediary (which enables its users to access online real money games) is required to implement methods to obtain parental consent before processing the personal data of a child and allowing access to the platform, respectively.

An online gaming intermediary means an intermediary that enables the users of its computer resource to access one or more online games.

An online real money game means an online game where a user makes a deposit in cash or kind with the expectation of earning winnings on that deposit.

Explanation - Winnings mean any prize, in cash or kind, which is distributed or intended to be distributed to a user of an online game based on the performance of the user and in accordance with the rules of such online game.

- 5. Are there legal remedies for children who have been victimized by online child sexual exploitation? This may include children who are victimized by the distribution of child pornography or CSAM imagery in which they are depicted, or children victimized by enticement, grooming or sextortion. If such legal remedies exist, do they include:**
- a. The ability to stop the publication of the pornography or CSAM imagery by the Online Platform?**
1. Rule 3(2)(b) (Due Diligence by an Intermediary) of the Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf
- Grievance redressal mechanism of intermediary:
- The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it.
2. Section 6 (Consent) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>
 - (1) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.
 - (2) Any part of consent referred in Sub-Section (1) which constitutes an infringement of the provisions of this Act or the rules made thereunder or any other law for the time being in force shall be invalid to the extent of such infringement.
 - (3) Every request for consent under the provisions of this Act or the rules made thereunder shall be presented to the Data Principal in a clear and plain language,

- giving her the option to access such request in English or any language specified in the Eighth Schedule to the Constitution and providing the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of this Act.
- (4) Where consent given by the Data Principal is the basis of processing of personal data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given.
 - (5) The consequences of the withdrawal referred to in Sub-Section (4) shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.
 - (6) If a Data Principal withdraws her consent to the processing of personal data under Sub-Section (5), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing the personal data of such Data Principal unless such processing without her consent is required or authorised under the provisions of this Act or the rules made thereunder or any other law for the time being in force in India.
 - (7) The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.
 - (8) The Consent Manager shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed.
 - (9) Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed.
 - (10) Where a consent given by the Data Principal is the basis of processing of personal data and a question arises in this regard in a proceeding, the Data Fiduciary shall be obliged to prove that a notice was given by her to the Data Principal and consent was given by such Data Principal to the Data Fiduciary in accordance with the provisions of this Act and the rules made thereunder.

Please note that:

- a) Section 2(i) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>, defines 'data fiduciary' as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
- b) Section 2(j) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>, defines 'data principal' as an individual to whom the personal data relates and where such individual is -
 - (i) a child, includes the parents or lawful guardian of such a child;
 - (ii) a person with disability, includes her lawful guardian, acting on her behalf.
- c) Section 2(w) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>, defines 'Processing', in relation to personal data, to mean a wholly or partly automated operation or set of



operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

- d) Section 2(t) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>, defines 'Personal data' as any data about an individual who is identifiable by or in relation to such data.
- e) Section 2(g) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf>, defines 'Consent Manager' as a person registered with the Data Protection Board of India, who acts as a single point of contact to enable a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

[Trilegal Note: The Digital Personal Data Protection Act, 2023 (DPDPA) has been passed by both the houses of legislature and assented to by the President of India and is currently awaiting notification by the government in the official gazette. The aforementioned provision will come into effect once the DPDPA is notified.]

- 3. Section 12 (Right to Correction and Erasure of Personal Data) of the Digital Personal Data Protection Act, 2023, available at <https://egazette.gov.in/WriteReadData/2023/247847.pdf> -
 - (1) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of Section 7, in accordance with any requirement or procedure under any law for the time being in force.
 - (2) A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal, -
 - (a) correct the inaccurate or misleading personal data;
 - (b) complete the incomplete personal data; and
 - (c) update the personal data.
 - (3) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

[Trilegal Note: The Digital Personal Data Protection Act, 2023 (DPDPA) has been passed by both the houses of legislature and assented to by the President of India and is currently awaiting notification by the government in the official gazette. The aforementioned provision will come into effect once the DPDPA is notified.]

b. An obligation on the part of the Online Platform to take active steps to remove the pornography or other imagery from their servers?

- 1. Rule 3(1)(b) (Due Diligence by an Intermediary) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at



https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The intermediary shall inform its rules and regulations, privacy policy and user agreement to the user in English or any language specified in the Eighth Schedule to the Constitution in the language of his choice and shall make reasonable efforts by itself, and to cause the users of its computer resource to not host, display, upload, modify, publish, transmit, store, update or share any information that, -

- (i) belongs to another person and to which the user does not have any right;
- (ii) is obscene, pornographic, paedophilic, invasive of another's privacy including bodily privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or an online game that causes user harm, or promoting enmity between different groups on the grounds of religion or caste with the intent to incite violence;
- (iii) is harmful to child;
- (iv) infringes any patent, trademark, copyright or other proprietary rights;
- (v) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature or, in respect of any business of the Central Government, is identified as fake or false or misleading by such fact check unit of the Central Government as the Ministry may, by notification published in the Official Gazette, specify;
- (vi) impersonates another person;
- (vii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting other nation;
- (viii) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
- (ix) is in the nature of an online game that is not verified as a permissible online game;
- (x) is in the nature of advertisement or surrogate advertisement or promotion of an online game that is not a permissible online game, or of any online gaming intermediary offering such an online game;
- (xi) violates any law for the time being in force.

Explanation - In this clause, "user harm" and "harm" mean any effect which is detrimental to a user or child, as the case may be.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

2. Rule 3(1)(c) (Due Diligence by an Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf



An intermediary shall periodically inform its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be.

[Trilegal Note: According to Rule 3(1)(b) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, an intermediary is required to undertake the following measures:

The rules and regulations, privacy policy or user agreement of the intermediary shall inform the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that, —

- (i) belongs to another person and to which the user does not have any right;
- (ii) is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;
- (iii) is harmful to child;
- (iv) infringes any patent, trademark, copyright or other proprietary rights;
- (v) violates any law for the time being in force;
- (vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;
- (vii) impersonates another person;
- (viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation;
- (ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
- (x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person.

Further, as per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

3. Rule 3(1)(d) (Due Diligence by an Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

An intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency



under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force:

Provided that any notification made by the Appropriate Government or its agency in relation to any information which is prohibited under any law for the time being in force shall be issued by an authorised agency, as may be notified by the Appropriate Government:

Provided further that if any such information is hosted, stored or published, the intermediary shall remove or disable access to that information, as early as possible, but in no case later than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency, as the case may be:

Provided also that the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under clause (b) on a voluntary basis, or on the basis of grievances received under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a) or (b) of sub-section (2) of section 79 of the Act.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

4. Rule 3(2)(b) (Due Diligence by an Intermediary) of the Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780732_4077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

Grievance redressal mechanism of intermediary:

The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it.

5. Rule 4(4) (Additional Due Diligence to be Observed by Significant Social Media Intermediary) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, available at



https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:

Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:

Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this sub-rule, including a periodic review of any automated tools deployed by such intermediary:

Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.

6. Section 79 (Exemption from Liability of Intermediary in Certain Cases) of the Information Technology Act, 2000, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077§ionId=13094§ionno=67B&orderno=85

- (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
- (2) The provisions of sub-section (1) shall apply if -
 - (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
 - (b) the intermediary does not -
 - (i) initiate the transmission,
 - (ii) select the receiver of the transmission, and
 - (iii) select or modify the information contained in the transmission;
 - (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.



(3) The provisions of sub-section (1) shall not apply if -

- (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
- (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation - For the purposes of this section, the expression 'third party information' means any information dealt with by an intermediary in his capacity as an intermediary.

c. An ability to get an injunction or other court order against the Online Platform to stop them from publishing the pornography or imagery?

1. Order 39, Rule 2 (Injunction to Restrain Repetition or Continuance of Breach) of the Code of Civil Procedure, 1908, available at <https://www.indiacode.nic.in/bitstream/123456789/2191/1/A1908-05.pdf>

(1) In any suit for restraining the defendant from committing a breach of contract or other injury of any kind, whether compensation is claimed in the suit or not, the plaintiff may, at any time after the commencement of the suit, and either before or after judgment, apply to the court for a temporary injunction to restrain the defendant from committing the breach of contract or injury complained of, or any breach of contract or injury of a like kind arising out of the same contract or relating to the same property or right.

(2) The court may by order grant such injunction, on such terms as to the duration of the injunction, keeping an account, giving security, or otherwise, as the court thinks fit.

2. Section 33(9) (Procedure and Powers of Special Court) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686&orderno=3

Subject to the provisions of this Act, a Special Court shall, for the purpose of the trial of any offence under this Act, have all the powers of a Court of Session and shall try such offence as if it were a Court of Session, and as far as may be, in accordance with the procedure specified in the Code of Criminal Procedure, 1973 (2 of 1974) for trial before a Court of Session.

[Trilegal Note: As per Section 28(2) (Sentences which High Courts and Sessions Judges may Pass) of the Code of Criminal Procedure, 1973, available at https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf, a sessions judge or additional sessions judge may pass any sentence authorised by law; but any sentence of death passed by any such judge shall be subject to confirmation by the High Court.]

3. Section 46 (Power to Adjudicate) of the Information Technology Act, 2000, available at



https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077§ionId=13094§ionno=67B&orderno=85

(1) For the purpose of adjudging under this Act whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder which renders him liable to pay penalty or compensation the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for damage does not exceed rupees five crore.

Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crores shall vest with the competent court.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the appellate tribunal under sub-section (2) of Section 58, and -
(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code (45 of 1860);
(b) shall be deemed to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974);
(c) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code 1908 (5 of 1908).

[Trilegal Note: As per Section 58(2) (Procedure and Powers of the Appellate Tribunal) of the Information Technology Act, 2000, the appellate tribunal shall have, for the purposes of discharging its functions under the Information Technology Act, 2000, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely: (a) summoning and enforcing the attendance of any person and examining him on oath; (b) requiring the discovery and production of documents or other electronic records; (c) receiving evidence on affidavits;



(d) issuing commissions for the examination of witnesses or documents; (e) reviewing its decisions; (f) dismissing an application for default or deciding it ex parte; and (g) any other matter which may be prescribed.

As per Section 151 (Saving of Inherent Powers of Court) of the Code of Civil Procedure, 1908, nothing in the Code of Civil Procedure, 1908, shall be deemed to limit or otherwise affect the inherent power of the court to make such orders as may be necessary for the ends of justice or to prevent abuse of the process of the court.]

d. A protective order or other court order that prohibits the person who posts the pornography or imagery from doing so in the future on the same or other Online Platform?

1. Order 39, Rule 2 (Injunction to Restrain Repetition or Continuance of Breach) of the Code of Civil Procedure, 1908, available at <https://www.indiacode.nic.in/bitstream/123456789/2191/1/A1908-05.pdf>

(1) In any suit for restraining the defendant from committing a breach of contract or other injury of any kind, whether compensation is claimed in the suit or not, the plaintiff may, at any time after the commencement of the suit, and either before or after judgment, apply to the court for a temporary injunction to restrain the defendant from committing the breach of contract or injury complained, of, or any breach of contract or injury of a like kind arising out of the same contract or relating to the same property or right.

(2) The court may by order grant such injunction, on such terms as to the duration of the injunction, keeping an account, giving security, or otherwise, as the court thinks fit.

2. Section 33(9) (Procedure and Powers of Special Court) of the Protection of Children from Sexual Offences Act, 2012, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_13_14_00005_201232_1517807323686&orderno=3

Subject to the provisions of this Act, a Special Court shall, for the purpose of the trial of any offence under this Act, have all the powers of a Court of Session and shall try such offence as if it were a Court of Session, and as far as may be, in accordance with the procedure specified in the Code of Criminal Procedure, 1973 (2 of 1974) for trial before a Court of Session.

[Trilegal Note: As per Section 28(2) (Sentences which High Courts and Sessions Judges may Pass) of the Code of Criminal Procedure, 1973, available at https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf, a sessions judge or additional sessions judge may pass any sentence authorised by law; but any sentence of death passed by any such judge shall be subject to confirmation by the High Court.]

3. Section 46 (Power to Adjudicate) of the Information Technology Act, 2000, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077§ionId=13094§ionno=67B&orderno=85



(1) For the purpose of adjudging under this Act whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder which renders him liable to pay penalty or compensation the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for damage does not exceed rupees five crore.

Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crores shall vest with the competent court.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

...

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the appellate tribunal under sub-section (2) of Section 58, and -
(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code (45 of 1860);
(b) shall be deemed to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974);
(c) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code 1908 (5 of 1908).

[Trilegal Note: As per Section 58(2) (Procedure and Powers of the Appellate Tribunal) of the Information Technology Act, 2000, the appellate tribunal shall have, for the purposes of discharging its functions under the Information Technology Act, 2000, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely: (a) summoning and enforcing the attendance of any person and examining him on oath; (b) requiring the discovery and production of documents or other electronic records; (c) receiving evidence on affidavits; (d) issuing commissions for the examination of witnesses or documents; (e) reviewing its decisions; (f) dismissing an application for default or deciding it ex parte; and (g) any other matter which may be prescribed.

As per Section 151 (Saving of Inherent Powers of Court) of the Code of Civil Procedure, 1908, nothing in the Code of Civil Procedure, 1908, shall be deemed to limit or otherwise affect the inherent power of the court to make such orders as may be necessary for the ends of justice or to prevent abuse of the process of the court.]

e. the ability to seek financial damages or any sort of monetary recovery from an offender



who has shared the child's image or video, either in a civil or a criminal proceeding?

1. Section 33(8) (Procedure and Powers of Special Courts) of the Protection of Children from Sexual Offences Act, 2012, available at <https://www.indiacode.nic.in/bitstream/123456789/2079/1/AA2012-32.pdf>

In appropriate cases, the Special Court may, in addition to the punishment, direct payment of such compensation as may be prescribed to the child for any physical or mental trauma caused to him or for immediate rehabilitation of such child.

2. Rules 9(1) and 9(2) (Compensation) of the Protection of Children from Sexual Offences Rules, 2020, available at <https://wcd.nic.in/acts/protection-children-sexual-offences-rules-2020>
 - (1) The Special Court may, in appropriate cases, on its own or on an application filed by or on behalf of the child, pass an order for interim compensation to meet the needs of the child for relief or rehabilitation at any stage after registration of the first information report. Such interim compensation paid to the child shall be adjusted against the final compensation, if any.
 - (2) The Special Court may, on its own or on an application filed by or on behalf of the victim, recommend the award of compensation where the accused is convicted, or where the case ends in acquittal or discharge, or the accused is not traced or identified, and in the opinion of the Special Court the child has suffered loss or injury as a result of that offence.
3. Section 357A (Victim Compensation Scheme) of the Code of Criminal Procedure, 1973, available at https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf
 - (1) Every State Government in co-ordination with the Central Government shall prepare a scheme for providing funds for the purpose of compensation to the victim or his dependents who have suffered loss or injury as a result of the crime and who require rehabilitation.
 - (2) Whenever a recommendation is made by the Court for compensation, the District Legal Service Authority or the State Legal Service Authority, as the case may be, shall decide the quantum of compensation to be awarded under the scheme referred to in sub-section (1).
 - (3) If the trial court, at the conclusion of the trial, is satisfied, that the compensation awarded under section 357 is not adequate for such rehabilitation, or where the cases end in acquittal or discharge and the victim has to be rehabilitated, it may make recommendation for compensation.
 - (4) Where the offender is not traced or identified, but the victim is identified, and where no trial takes place, the victim or his dependents may make an application to the State or the District Legal Services Authority for award of compensation.
 - (5) On receipt of such recommendations or on the application under sub-section (4), the State or the District Legal Services Authority shall, after due enquiry award adequate compensation by completing the enquiry within two months.
 - (6) The State or the District Legal Services Authority, as the case may be, to alleviate the suffering of the victim, may order for immediate first-aid facility or medical benefits to be made available free of cost on the certificate of the police officer not below the rank of the officer in charge of the police station or a Magistrate of



the area concerned, or any other interim relief as the appropriate authority deems fit.

[Trilegal Note: The Bhartiya Nagarik Suraksha Sanhita, 2023 (BNSS) has been passed by both the houses of legislature and assented to by the President of India and will come into force on 01 July 2024. Once the BNSS is notified, the Code of Criminal Procedure, 1973 will be repealed and Section 396 of the BNSS will apply with certain changes.]

4. Rule 4(1)(a) of the Haryana Victim Compensation Scheme, 2020, available at <https://cdnbbsr.s3waas.gov.in/s3100d9f30ca54b18d14821dc88fea0631/uploads/2022/10/2022100631.pdf>

A victim shall be eligible for the grant of compensation where, a recommendation is made by the Court under sub-sections (2) and (3) of Section 357A of the Act, if no recommendation is made by the trial court, no compensation shall be granted by District Legal Services Authority except in the case when the offender is not traced out or identified.

5. Rule 5(1)(a) of the Himanchal Pradesh (Victim of Crime) Compensation Scheme, 2019, available at https://himachal.nic.in/showfile.php?lang=1&dpt_id=240&level=1&lid=19377&sublinkid=18896

(1) A victim shall be eligible for the grant of compensation –

(a) Where the trial Court, under sub-section (2) of Section 357A of the Code makes a recommendation or an application is made under sub-section (4) of Section 357A of the Code to the District or State Legal Services Authorities.

(b) Assistance under the scheme shall be available in respect of each of the cases where the F.I.R is lodged.

(c) Where the trial court, at the conclusion of the trial, is satisfied that the compensation awarded under Section 357 of the code is not adequate for such rehabilitation, or where the case ends in acquittal or discharge and the victim has to be rehabilitated and a recommendation by the Court for compensation is made:

Provided that the victim, within reasonable time frame, gives information to the officer-in-charge of a police station of the commission of crime within the limits of such station or to a Judicial Magistrate empowered to take cognizance of such offence arising out of the crime:

Provided further that the victim co-operates with the police and prosecution during investigation and trial of the case:

Provided further that the application is made on Annexure I to the District Legal Services Authority of the District where the crime was committed (for award of compensation as provided in sub-section (4) of section 357A of



the code).

6. Rule 4 (Victim Compensation Fund) of the West Bengal Victim Compensation Scheme, 2017, available at <https://wbslsa.bangla.gov.in/#legislations>

Where the offender is not traced or identified, but the victim is identified, and where no trial takes place, the victim or his/her dependents may make an application to the State or the District Legal Services Authority for award of compensation if, -

- (a) he/she has not been compensated for the loss or injury under any other Scheme of the Central or State government, insurance company or any other institution,
 - (b) the loss or injury sustained by the victim has caused substantial loss of income to his/her family making it difficult to meet their both ends without any compensation.
7. Rule 6 (Criteria for Grant of Compensation) of the Punjab Victim Compensation Policy, available at https://pulsa.punjab.gov.in/sites/default/files/Punjab%20Victim%20compensation%20policy%202017_0_0.pdf

- (1) The victims or his dependents may file applications which may be considered for the grant of compensation by the competent authority falling in any of the following categories -
 - (a) where a recommendation has been made by the Court under sub-section (2) or sub-section (3) of section 357-A of the Code;
 - (b) where the offender is not traced/traceable or identified, but the victim is identified and where no trial takes place and the victim has to incur expenses on physical and mental rehabilitation, and the victim or his dependent makes an application to the Punjab Legal Services Authority or the District Legal Services Authority;
 - (c) where the Punjab Legal Services Authority or the District Legal Service Authority, as the case may be, in order to alleviate the suffering of the victim, orders for immediate first-aid facility or medical aid to be made available to him, free of cost, on the certificate of the police officer concerned not below the rank of the officer-in-charge of the police station or a Magistrate of the area concerned, or any other interim relief as the said authorities may deem fit.
- (2) The applications for the grant of compensation may be considered by the Punjab Legal Services Authority or the District Legal Services Authority, subject to the following-
 - (a) the victim or his dependent should not have compensated for such loss or injury under any other scheme of the Central Government or Punjab Government except where any relief has been granted under the following schemes:
 - (i) Prime Minister's National Relief Fund (PMNRF);
 - (ii) Central Victims Compensation Scheme (CVCS);
 - (iii) Chief Minister Relief Fund;
 - (iv) the Punjab Financial Assistance to Acid Victims Scheme 2017 of the Department of Social Security and Department of Development of Women and Child of the Government of Punjab; and



- (v) any other scheme or funds which provides for relief in addition to the Victims Compensation Scheme under Section 357-A of the Code;
- (b) The crime, on account of which the compensation is to be paid under this Scheme, should have been occurred within the State.

Exception: - In case, the crime has occurred outside the State and the victim is found within the limit of the State, he shall be eligible for interim relief contemplated under sub-section (6) of Section 357-A of the Code.

8. Rule 4 of the Jharkhand Victim Compensation Scheme, 2012, available at https://jhalsa.org/pdfs/Reading_Materials/compendium.pdf

A Victim shall be eligible for the grant of compensation if, -

- (a) the offender is not traced or identified, but the victim is identified, and where no trial takes place, such victim may also apply grant of compensation under sub section (4) of section 357-A of the Act;
 - (b) the victim/claimant report the crime to the officer-in-charge of the police station within 48 hours of the occurrence or any senior police officer or Executive Magistrate or Judicial Magistrate of the area provided that the District Legal Services Authority, if satisfied, for the reasons to be recorded in writing, may condone the delay in reporting;
 - (c) the victim/ claimant cooperate with the police and prosecution during the investigation and trial of the case.
9. Rule 4 of the Assam Victim Compensation Scheme, available at <https://aslsa.assam.gov.in/portlets/victim-compensation>

The victim or his dependents satisfying the following criterion shall be eligible for grant of the compensation:

- (1) Loss or injury sustained by the victim or his dependents should have caused substantial loss to the income of the family making it difficult to meet their both ends without the financial aid or has to spend beyond his means on medical treatment of mental/physical injury and a recommendation is made by the Court for compensation.
 - (2) The victim/dependents report the crime to the officer-in-charge of police station or judicial magistrate of the area promptly, provided that the District Legal Services Authority, if satisfied, for the reasons to be recorded in writing, may condone the delay in reporting.
 - (3) The victim/dependents co-operates with the police and prosecution during the investigation and trial of the case.
 - (4) Where the perpetrator of heinous crime is not traceable or goes unpunished after trial, but the victim is identified and the victim has to be rehabilitated physically and mentally, such victim may also apply for grant of compensation under sub-section (4) of Section 357-A of the Act.
- f. **the ability to seek any other forms of victim compensation/recovery/services provided for under the law and/or by a government-funded source?**

1. Section 19(5) (Reporting of Offences) of the Protection of Children from Sexual Offences



Act, 2012, available at

<https://www.indiacode.nic.in/bitstream/123456789/2079/1/AA2012-32.pdf>

Where the Special Juvenile Police Unit or local police is satisfied that the child against whom an offence has been committed is in need of care and protection, then, it shall, after recording the reasons in writing, make immediate arrangement to give him such care and protection (including admitting the child into shelter home or to the nearest hospital) within twenty-four hours of the report, as may be prescribed.

2. Rule 4(4) (Procedure Regarding Care and Protection of Child) of the Protection of Children from Sexual Offences Rules, 2020, available at
<https://wcd.nic.in/acts/protection-children-sexual-offences-rules-2020>

Where the Special Juvenile Police Unit or the local police receives information under sub-section (1) of section 19 of the Act, and has a reasonable apprehension that the offence has been committed or attempted or is likely to be committed by a person living in the same or shared household with the child, or the child is living in a child care institution and is without parental support, or the child is found to be without any home and parental support, the concerned SJPU, or the local police shall produce the child before the concerned Child Welfare Committee (hereafter referred to as "CWC") within 24 hours of receipt of such report, together with reasons in writing as to whether the child is in need of care and protection under sub-section (5) of section 19 of the Act, and with a request for a detailed assessment by the CWC.

3. Rule 4(8) (Procedure Regarding Care and Protection of Child) of the Protection of Children from Sexual Offences Rules, 2020, available at
https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf

The Child Welfare Committee, on receiving a report under sub-section (6) of section 19 of the Act or on the basis of its assessment made under sub-rule (5), and with the consent of the child and child's parent or guardian or other person in whom the child has trust and confidence, may provide a support person to render assistance to the child in all possible manner throughout the process of investigation and trial, and shall immediately inform the SJPU or Local Police about providing a support person to the child.

4. Rule 4(12) (Procedure Regarding Care and Protection of Child) of the Protection of Children from Sexual Offences Rules, 2020, available at
https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf

The Child Welfare Committee shall also seek monthly reports from support person till the completion of trial, with respect to condition and care of child, including the family situation focusing on the physical, emotional and mental well-being, and progress towards healing from trauma; engage with medical care facilities, in coordination with the support person, to ensure need-based continued medical support to the child, including psychological care and counseling; and shall ensure resumption of education of the child, or continued education of the child, or shifting of the child to a new school, if required.

5. Rule 4(14) (Procedure Regarding Care and Protection of Child) of the Protection of Children from Sexual Offences Rules, 2020, available at



https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf

Special Juvenile Police Unit or the local police shall also inform the child and child's parents or guardian or other person in whom the child has trust and confidence about their entitlements and services available to them under the Act or any other law for the time being applicable as per Form-A. It shall also complete the preliminary assessment report in Form B within 24 hours of the registration of the First Information Report and submit it to the Child Welfare Committee.

As per Form A of the Protection of Children from Sexual Offences Rules, 2020, available at <https://wcd.nic.in/acts/protection-children-sexual-offences-rules-2020>, children who have suffered sexual abuse are entitled to receive the following:

- a) To receive a copy of the FIR.
 - b) To receive adequate security and protection by police.
 - c) To receive immediate and free medical examination by civil hospital/PHC etc.
 - d) To receive counseling and consultation for mental and psychological well being
 - e) For recording of statement of child by woman police officer at child's home or any other place convenient to child
 - f) To be moved to a child care institution where offence was at home or in a shared household, to the custody of a person whom child reposes faith.
 - g) For immediate aid and assistance on the recommendation of CWC.
 - h) For being kept away from accused at all times, during trial and otherwise.
 - i) To have an interpreter or translator, where needed.
 - j) To have special educator for the child or other specialized person where child is disabled.
 - k) For free legal aid.
 - l) For support person to be appointed by child welfare committee.
 - m) To continue with education.
 - n) To privacy and confidentiality.
 - o) For list of important contact no.'s including that of the District Magistrate and the Superintendent of Police.
6. Rule 7 (Legal Aid and Assistance) of the Protection of Children from Sexual Offences Rules, 2020, available at https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf
- (1) The Child Welfare Committee shall make a recommendation to District Legal Services Authority (hereafter referred to as "DLSA") for legal aid and assistance.
 - (2) The legal aid and assistance shall be provided to the child in accordance with the provisions of the Legal Services Authorities Act, 1987 (39 of 1987).
7. Rule 8 (Special Relief) of the Protection of Children from Sexual Offences Rules, 2020, available at https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf
- (1) For special relief, if any, to be provided for contingencies such as food, clothes, transport and other essential needs, CWC may recommend immediate payment of such amount as it may assess to be required at that stage, to any of the following:-
 - (i) the DLSA under Section 357A; or;
 - (ii) the DCPU out of such funds placed at their disposal by state or;

- (iii) funds maintained under section 105 of the Juvenile Justice (Care and Protection of Children) Act, 2015 (2 of 2016);
- (2) Such immediate payment shall be made within a week of receipt of recommendation from the CWC.

[Trilegal Note: As per Section 105(1) of the Juvenile Justice (Care and Protection of Children) Act, 2015, the State Government may create a fund in such name as it thinks fit for the welfare and rehabilitation of the children dealt with under the Act.]

g. notification to a victim when an offender is arrested for distributing child pornography or CSAM in which the child is depicted?

Rule 4(15) (Procedure Regarding Care and Protection of Child) of the Protection of Children from Sexual Offences Rules, 2020, available at https://wcd.nic.in/sites/default/files/POCSO%20Rules%20merged_0.pdf

The information to be provided by the SJPU, local police, or support person, to the child and child's parents or guardian or other person in whom the child has trust and confidence, includes but is not limited to the following:

- (i) the availability of public and private emergency and crisis services;
- (ii) the procedural steps involved in a criminal prosecution;
- (iii) the availability of victim's compensation benefits;
- (iv) the status of the investigation of the crime, to the extent it is appropriate to inform the victim and to the extent that it will not interfere with the investigation;
- (v) the arrest of a suspected offender;
- (vi) the filing of charges against a suspected offender;
- (vii) the schedule of court proceedings that the child is either required to attend or is entitled to attend;
- (viii) the bail, release or detention status of an offender or suspected offender;
- (ix) the rendering of a verdict after trial; and
- (x) the sentence imposed on an offender.

6. "Safety by Design" is defined as tools or processes that are built into an Online Platform to protect children by making it easier for the relevant Online Platform to detect or prevent the distribution of child pornography or CSAM.

a. Are Online Platforms legally required to incorporate "Safety by Design" into their systems?

Yes

i. If so, must these steps be taken before the launch of an Online Platform?

Yes

ii. If so, if an Online Platform has already been in public use, when must they have incorporated "Safety by Design" measures?

As per the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, if a social media intermediary crosses the prescribed



threshold of number of registered users in India, it may be deemed as a significant social media intermediary and be required to comply with certain additional requirements (specified in 6(a)(iii) below).

[Trilegal Note: A significant social media intermediary means a social media intermediary (i.e., an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services) having fifty lakh registered users in India.]

iii. For each of 6(a)(i) or (ii) above, please describe the legal requirement or recommendation.

A. Legal requirements for 6(a)(i) -

1. Rule 3(1)(b) (Due Diligence by an Intermediary) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The intermediary shall inform its rules and regulations, privacy policy and user agreement to the user in English or any language specified in the Eighth Schedule to the Constitution in the language of his choice and shall make reasonable efforts by itself, and to cause the users of its computer resource to not host, display, upload, modify, publish, transmit, store, update or share any information that, -

- (i) belongs to another person and to which the user does not have any right;
- (ii) is obscene, pornographic, paedophilic, invasive of another's privacy including bodily privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or an online game that causes user harm, or promoting enmity between different groups on the grounds of religion or caste with the intent to incite violence;
- (iii) is harmful to child;
- (iv) infringes any patent, trademark, copyright or other proprietary rights;
- (v) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature or, in respect of any business of the Central Government, is identified as fake or false or misleading by such fact check unit of the Central Government as the Ministry may, by notification published in the Official Gazette, specify;
- (vi) impersonates another person;

- (vii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting other nation;
- (viii) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
- (ix) is in the nature of an online game that is not verified as a permissible online game;
- (x) is in the nature of advertisement or surrogate advertisement or promotion of an online game that is not a permissible online game, or of any online gaming intermediary offering such an online game;
- (xi) violates any law for the time being in force.

Explanation - In this clause, "user harm" and "harm" mean any effect which is detrimental to a user or child, as the case may be.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

2. Rule 4A(3) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The online gaming self-regulatory body, upon an application made to it by its member in respect of an online real money game, may declare such online real money game as a permissible online real money game, if, after making such inquiry as it deems fit, it is satisfied that -

- (a) the online real money game does not involve wagering on any outcome; and
- (b) the online gaming intermediary and such online game is in compliance with the provisions of rules 3 and 4, the provisions of any law relating to the age at which an individual is competent to enter into a contract, and the framework made by the online gaming self-regulatory body under sub-rule (8):

Provided that an online gaming self-regulatory body may, initially rely upon the information furnished by the applicant for verification of the online real money game and declare such game as a permissible online real money game for a period not exceeding three months:

Provided further that the online gaming self-regulatory body shall endeavour to complete the inquiry within the said period of three months and, upon its completion, either declare the online real money game as a permissible online real money game or inform the applicant in writing with the reasons thereof that such online game does not meet the requirements under these rules.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

3. Rule 4A(8) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The online gaming self-regulatory body shall prominently publish on its website, mobile based application or both, as the case may be, a framework for verifying an online real money game, which, among other things, includes the following, namely -

- (a) the measures to ensure that such online real money game is not against the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States and public order;
- (b) the safeguards against user harm, including self-harm and psychological harm;
- (c) the measures to safeguard children, including measures for parental or access control and classifying online games through age-rating mechanism, based on the nature and type of content; and
- (d) the measures to safeguard users against the risk of gaming addiction, financial loss and financial fraud, including repeated warning messages at higher frequency beyond a reasonable duration for a gaming session and provision to enable a user to

exclude himself upon user-defined limits being reached for time or money spent.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3 online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

B. Legal requirements for 6(a)(ii) -

Rule 4(1)(a) (Additional Due Diligence to be Observed by Significant Social Media Intermediary and Online Gaming Intermediary) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

In addition to the due diligence observed under Rule 3, a significant social media intermediary, within three months from the date of notification of the threshold under clause (v) of sub-rule (1) of Rule 2, and an online gaming intermediary that enables the users to access any permissible online real money game, shall observe the following additional due diligence while discharging its duties, namely -

- (a) appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and rules made thereunder and shall be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary or such online gaming intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Act and rules made thereunder:

Provided that no liability under the Act or rules made thereunder may be imposed on such significant social media intermediary without being given an opportunity of being heard.

Explanation - For the purposes of this clause "Chief Compliance Officer" means a key managerial personnel or such other senior employee of a significant social media intermediary or an online gaming intermediary, as the case may be, who is resident in India.

[Trilegal Note: As per Rule 4B of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the obligations under this provision will not apply to online gaming intermediaries until the expiry of 3 months from the date on which the government notifies at least 3



online gaming self-regulatory bodies. Please note that online gaming self-regulatory bodies have not been notified yet.]

b. Please include information about the parameters for monitoring, management, and enforcement of any legal or regulatory requirements for the Online Platform's incorporation of "Safety by Design"?

1. Rule 7 (Non-Observance of Rules) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the Information Technology Act, 2000 shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Information Technology Act, 2000 and the Indian Penal Code.

[Trilegal Note: Please note that Section 79 (Exemption from Liability of Intermediary in Certain Cases) of the Information Technology Act, 2000, available at https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077§ionId=13094§ionno=67B&orderno=85, provides as follows:

- (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
- (2) The provisions of sub-section (1) shall apply if -
 - (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
 - (b) the intermediary does not-
 - (i) initiate the transmission,
 - (ii) select the receiver of the transmission, and
 - (iii) select or modify the information contained in the transmission;
 - (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
- (3) The provisions of sub-section (1) shall not apply if -
 - (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
 - (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource



without vitiating the evidence in any manner.

Explanation - For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.]

2. Rule 4A(4) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The online gaming self-regulatory body shall publish and maintain on its website, mobile based application or both, at all times, an updated list of all permissible online real money games verified under sub-rule (3), along with the details of such online games including the details of the applicant, the dates and period of validity of the verification, the reasons of such verification and the details of the suspension or revocation, if any, of verification of any online real money game.

3. Rule 4A(7) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The online real money game verified under sub-rule (3), and the online gaming intermediary which enables access to such online real money game, shall display a demonstrable and visible mark of such verification stating that the online real money game is verified by the online gaming self-regulatory body as a permissible online real money game under these rules.

4. Rule 4A(9) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The Ministry may, if it considers it necessary, by a notice in writing, require an online gaming self-regulatory body to furnish to the Ministry or disclose on such body's website or mobile based application or both, such information as the Ministry may specify in the notice.

5. Rule 4A(12) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

Where the Ministry is of the view that any verification of a permissible online real money game by an online gaming self-regulatory body is not in conformity with these rules, it may, after giving such body an opportunity of being heard, communicate, in writing, the fact of such non-conformity to that body and direct it to take measures to rectify the same.



6. Rule 4A(13) (Verification of Online Real Money Game) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=intermediary_guidelines-dmec_rules_25-02-2021.pdf

The Ministry may, if it is satisfied that it is necessary so to do, after giving the online gaming self-regulatory body an opportunity of being heard, by order, for reasons to be recorded in writing, suspend or revoke the designation of such body:

Provided that the Ministry may, in the interest of the users of any online game that was verified by such body at the same time or at any subsequent time, give such interim directions as it may deem necessary to any intermediary or class of intermediaries regarding enabling its users to access such online game.