



PLEASE NOTE THAT THE RESEARCH INFORMATION CONTAINED IN THIS DOCUMENT IS BASED SOLELY ON A REVIEW OF PUBLICLY AVAILABLE SOURCES AND WITHOUT ASSISTANCE FROM LICENSED LEGAL PROFESSIONALS IN THE RELEVANT JURISDICTION. IT DOES NOT CONSTITUTE LEGAL ADVICE AND IT SHOULD NOT BE RELIED UPON AS SUCH. TO THE EXTENT LEGAL ADVICE MAY BE REQUIRED, IT SHOULD BE OBTAINED FROM LICENSED LEGAL PRACTITIONERS IN THE RELEVANT JURISDICTION. *The responses for this country are provided for informational purposes only. 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 from the law firm that prepared them.*

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>)

Section 2 of the Custody, Contact, Guardianship and Maintenance Act, 2011 (parliament.gov.gy), defines “child” as “a person under the age of eighteen years, whether born in or out of wedlock who has never been married and includes –

- (a) a stepchild;
- (b) a child adopted by law;
- (c) a child of the family, except that in the case where a person has special needs, that person shall be considered a child under this Act regardless of the person's age.”

The Act defines “minor” as “a person who is under eighteen years of age.”

Section 2 of the Childcare and Protection Agency Act, 2009 (mhsss.gov.gy), defines “child” as “a person under the age of eighteen years and shall also include a person who attains the age of eighteen years while under care or protection in accordance with any law or is, because of some disability, certified by the Director as being in need of care or protection on and after attaining that age for such period as may be specified by the Director.”

Section 2 of the Protection of Children Act, 2009 defines “child” as “a person under the age of eighteen years, whether born in or out of wedlock, who has never been married, and includes –

- (a) a stepchild or child adopted by law; or
- (b) a child of the family; except that in the case where a person has special needs that person shall be a child under this Act regardless of his age.”

Section 2 of the Cyber Crime Act, 2018, 17173-17173-act_no._16_of_2018_(1).pdf, defines “child” as “a person under the age of eighteen years.”

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>)

Not specifically defined.

“Abuse” includes “the sexual exploitation of a child, molestation of a child, or the involvement of a child in unlawful sexual activity, prostitution or pornography.”

Section 2 of the Childcare and Protection Agency Act, 2009.

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

Not specifically defined.

Section 2 of the Cyber Crime Act, 2018 defines “sexual activity” (in reference to what constitutes child pornography) to include “touching with any part of the body, which includes a part surgically constructed (in particular, through gender reassignment surgery), with anything else or through anything; or any other activity, if a reasonable person would consider that –

- (i) whatever its circumstances or any person's purpose in relation to it, it is because of its nature sexual; or
- (ii) because of its nature it may be sexual and because of its circumstances or the purpose of any person in relation to it (or both) it is sexual; or sexual intercourse.”

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

Not specifically defined.

“Abuse” includes “the sexual exploitation of a child, molestation of a child, or the involvement of a child in unlawful sexual activity, prostitution or pornography,” as well as “any other unlawful act likely to cause physical, psychological or emotional harm to a child.”

Section 2 of the Childcare and Protection Agency Act, 2009.

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

According to Section 2 of the Cyber Crime Act 2018, “child pornography”:

- (a) means any visual depiction, including any film, video, digital image, computer or computer-generated or modified image, animation or text, of –
 - (i) a child engaging in real or simulated explicit sexual activity;
 - (ii) a child in a sexually explicit pose;
 - (iii) parts of a child's body pasted, for sexual purposes, to visual representations of parts of an adult's body or vice versa;
- (b) does not include any visual representation of a child's body produced or reproduced for the purpose of education, counselling, or promotion of reproductive health or as part of a criminal investigation and prosecution or civil proceedings or in the lawful performance of a person's profession, duties and functions;
- (c) does not require proof of the actual identity of a child.”



- 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>)**

See response to 1(e) above. The Cybercrime Act defines child pornography to include “computer generated or modified images” of children engaging in sexual activity.

- 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>)**

Not specifically defined.

Section 13 of the Sexual Offences Act, 2010, criminalizes the offense of “meeting a child following sexual grooming,” which occurs if a person eighteen years of age or over:

- (1) (a) having met or communicated with another person (“the complainant”) on at least two earlier occasions, the accused:
 - (i) meets the complainant; or
 - (ii) travels with the intention of meeting the complainant in any part of the world;
 - (b) at the time, the accused intends to do anything to or in respect of the complainant, during or after the meeting and in any part of the world, which if done will involve the commission by the accused of an offence under this Act; and
 - (c) the complainant is under sixteen years of age and the accused does not reasonably believe that the complainant is sixteen years of age or over.
- (2) In subsection (1)(a) the reference to the accused having met or communicated with the complainant is a reference to the accused having met the complainant in any part of the world or having communicated with the complainant by any means from, to or in any part of the world.

Section 2:15 of the Cybercrimes Act defines the offense of “child luring” as follows:

A person commits an offence if the person uses a computer system to –

- (a) communicate with a child with the intent to induce the child to engage in sexual conversations or sexual activities; or
 - (b) arrange a meeting with a child with the intent of abusing or engaging in sexual activity with the child or producing child pornography, whether or not he takes any steps to effect such a meeting.
- h. legal age of consent for sexual activity – are there laws and regulations, if so, what ages are specified?**

Yes. General “age of consent” is 16 years old, under the Sexual Offences Act, 2010 (cepal.org), which criminalizes all sexual activity with a child below the age of 16.

Section 10 of the Sexual Offences Act, 2010 provides that:

- (1) A person (“the accused”) commits the offence of rape of a child under sixteen years of age (“the complainant”) if the accused –



- (a) engages in sexual penetration with the complainant; or
 - (b) causes the complainant to engage in sexual penetration with a third party.
- (2) It is irrelevant whether at the time of the penetration the accused believed the complainant to be sixteen years of age or over.

Section 11 of the Act provides:

- (1) A person ("the accused") commits the offence of sexual activity with a child under sixteen years of age ("the complainant") if the accused –
 - (a) engages in a sexual activity (not including sexual penetration) with a child who is under sixteen years of age;
 - (b) causes or incites the complainant to engage in a sexual activity with a third party; or
 - (c) causes the complainant to perform a sexual act including causing the complainant to masturbate.
 - (2) It is irrelevant whether at the time of the activity the accused believes the complainant to be sixteen years of age or over.
- 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>)**

Not defined.

Section 2:19:4 of the Cybercrime Act provides: "A person who uses a computer system with the intent to extort a benefit from another person by threatening to publish electronic data containing personal or private information which can cause the other person public ridicule, contempt, hatred or embarrassment commits an offence."

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**

Section 2:14 of the Cybercrime Act, 2018 provides:

- (1) A person commits an offence if the person intentionally –
 - (a) produces child pornography with the use of a computer system;
 - (b) offers or makes available, distributes or transmits child pornography through a computer system;
 - (c) procures or obtains child pornography through a computer system for himself or another person; or
 - (d) possesses child pornography in a computer system or on a computer data storage medium.
 - (2) A person or a service provider who has knowledge of another person committing child pornography through a computer system shall report the commission of the child pornography to the Police.
 - (3) A person or a service provider who fails to comply with subsection (2) commits an



offence.

A “service provider” is defined as “(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or (b) any public or private entity that processes or stores electronic data on behalf of such communication service or users of such service.”

Section 2:25 of the Cybercrime Act requires also service providers to store traffic data of subscribers for ninety days from the date the data is generated by a computer system. A service provider who fails to comply with this provision commits an offence and is liable up to a fine of three million dollars and to imprisonment for one year.

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

Section 2:15 of the Cybercrime Act provides:

...

(2) A person or a service provider who has knowledge of another person committing child luring through a computer system shall report the commission of the child luring to the Police.

(3) A person or service provider who fails to comply with subsection (2) commits an offence.

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

See responses to 2(a) and (b).

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

Section 2:37 of the Cybercrime Act provides:

A Judge, if satisfied on an ex parte application by a police officer of the rank of Superintendent or above that a service provider or any other entity with a domain name server is storing, transmitting or providing access to electronic data in contravention of this Act or any other written law, may order the service provider or other entity with a domain name server to remove, or disable access to, the electronic data.

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

N/A

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

See response to 2(d).



- 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.

N/A

- 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.?

N/A

- 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?

N/A

- 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?

N/A

- 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:

NO

- a. The ability to stop the publication of the pornography or CSAM imagery by the Online Platform?

None found.

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

None found.

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



None found.

- 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?

None found.

- 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?

None found.

- 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?

None found.

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

None found.

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?

N/A

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

N/A

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

N/A

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

N/A

- 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"?

None found.