Report on the results of the risk assessment for Pornhub.com pursuant to Article 34 of the Digital Services Act

Aylo Freesites Limited – April 2025

Pornhub.com ("**Pornhub**") is an online platform provided by Aylo Freesites Limited. The platform has been designated as a very large online platform according to Article 33 of the Digital Services Act (Regulation EU 2022/2065) by the European Commission on 20 December 2023. Pursuant to Article 34 of the Digital Services Act, Aylo has identified, analyzed and assessed systemic risks in the Union resulting from, or influenced by, the design and functioning of Pornhub.com and its related systems, including algorithmic systems, or from the use made of the service.

This report sets out the results of this risk assessment.

This report is authored by

Aylo Freesites Ltd,
Block 1,
195-197 Old Nicosia-Limassol Road,
Dali Industrial Zone,
Cyprus 2540

April 2025

Results

To assess each risk, Aylo has assigned a probability and severity level to each risk, using the following scales:

- **Severity:** 'negligible" to 'very critical'
- **Probability:** 'improbable' to 'frequent'.

The overall risk assessment is based on the following Probability-Severity-Matrix:

Probability	**Severity**			
	Slight	**Marginal**	**Critical**	**Very critical**
Frequent	High	High	Very high	Very high
Probable	Medium	High	High	Very high
Occasional	Low	Medium	High	Very high
Remote	Low	Medium	Medium	High
Improbable	Low	Low	Medium	Medium
Eliminated	Eliminated			

Aylo has conducted an in-depth risk assessment for Pornhub.com. The following table lists the most relevant risks as well as the results of the risk assessment using the scales introduced above:

Category	Risk	Severity	Probability	Risk
Dissemination of illegal content	Child sexual abuse material (CSAM)	Critical	Improbable	Medium
	Non-consensual content (NCC)	Marginal - Critical	Remote	Medium
	Doxing and harassment	Marginal - Critical	Occasional – Remote	Medium
	Copyright infringements	Marginal	Improbable	Low
	Terrorism	Critical	Improbable	Medium
	AI generated content representing illegal acts	Critical	Improbable	Medium
Fundamental rights	Hate speech, and fostering stereotypes regarding sexual preferences and behaviour	Critical	Remote	Medium
	Sex trafficking	Critical	Remote	Medium
	Data minimization	Critical	Remote	Medium
Civic Discourse, electoral process and public security	Politically provocative content and adverts	Critical	Improbable	Medium
	Deep fakes	Critical	Improbable	Medium
	Over-blocking	Slight	Improbable	Low
Gender based violence, public health, minors, physical and mental well-being	Negative effects in relation to minors	Slight – Marginal	Remote	Low – Medium
	Porn addiction	Slight – Marginal	Remote	Low - Medium
	Negative effects on relationships	Slight – Marginal	Remote	Low - Medium
	Pornography fostering abuse and violence	Critical	Improbable	Medium

	Frustration due to unrealistic expectations	Slight – Marginal	Remote	Low - Medium
Overarching factors	Ad Delivery	Critical	Improbable	Medium
	Recommender Systems	Critical	Improbable	Medium

Since all risk levels are in the range of medium to low because of the extensive risk mitigation measures Aylo has implemented, the residual risks do not require additional mitigation measures according to Article 35 of the Digital Services Act.

Summary of most relevant factors considered in the risk assessment for Pornhub pursuant to Article 34 of the Digital Services Act

Aylo Freesites Limited – April 2025

Table of contents

Dissemination of illegal content

Child sexual abuse material (CSAM)

Recital 80 of the DSA singles out CSAM dissemination as an example of a systemic risk, pointing out that such a dissemination may "constitute a significant systemic risk where access to illegal content may spread rapidly and widely through accounts with a particularly wide reach or other means of amplification".

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected viewers: Anyone who sees it. The reach depends upon how long the material remains on the site and the number of views – Critical
	Number of affected victims: The number of victims is very limited – Slight As our most recent voluntary (and separate from the mandatory DSA reporting) transparency report for the second half of 2024 shows, only a very small share of uploads contains CSAM and an even smaller share of those uploads were caught only after publication, and thus reached an audience on Pornhub. *"Of the videos uploaded and reported as potential CSAM in the second half of 2024, which represents 0.09% of videos uploaded during that period, 97.75% were removed before being viewed."* *"Videos uploaded in the last six months of 2024 and removed for violating our CSAM policy accounted for 0.001% of total views of all videos uploaded in that period."* Also note in the IWF Annual Report 2023, IWF found 275,652 URLs on the web confirmed to contain CSAM. In contrast, not a single piece of CSAM was found on Pornhub (or indeed on any other of Aylo's platforms) since the year 2021. The NCMEC reports regarding notifications sent by NCMEC to Responsive Service Providers (2021, 2022, 2023), demonstrates a leading position of Pornhub, with merely 1-3 notifications per year over the last three. To put this in context, popular online platforms often received 10-2500 notifications.

	The number of notifications received from NCMEC is low as a positive result of our ever-evolving trust & safety measures and our constantly intensifying collaboration with NGOs over the years. Potential use by minors who may have accessed Pornhub despite the clear prohibitions and access restrictions is also addressed with the mitigation measures we have in place. There could be an increased risk associated with minors searching for CSAM content, but mitigation measures reduce the likelihood of such material existing on the platform and the deterrence messaging makes clear that this material is unacceptable and warns children and adults alike of the consequences.
	Irreversibility of the damage: A removal can remedy, but will not remove the negative impact on those who saw it or those depicted in the content – Critical
Probability The likelihood of the risk materializing	**Improbable**
	It is highly unlikely that CSAM will be uploaded and disseminated on Pornhub due to the numerous mitigating measures in place. This is supported by statistics from our latest transparency report as referenced above.
Overall assessment	**Medium**

Mitigating measures in place

Policies

- The platform has a zero tolerance policy for any attempted CSAM uploads. Our CSAM policy makes this very clear.

Identity and consent

There are two types of uploaders on Pornhub: individual content creators, often referred to as "Models", and content partners, or third-party professional content studios.

As part of their registration, content partners are required to provide a company name, company/studio content website, and physical address or URL indicating the coordinates of their custodian of 2257 records (pursuant to the record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content).

Every new uploader is required to undergo identity verification with a third-party identity verification provider, which requires them to:

- Submit a government-issued ID, which is authenticated by the provider.
- Conduct a liveness test to ensure the users likeness matches the government-issued ID and they are one and the same person.
- The liveness test also ensures that the person is alive and real, not AI, not pre-recorded, not a still image.

At time of signup, and again at the time of each upload, all uploaders are required to attest that they have obtained and retained ID and consent to record and distribute content from all other performers appearing in their content.

As part of Pornhub's more extensive verification processes, for individual content creators these requirements are validated at least once per additional performer:

- Uploaders may meet the ID and consent verification requirement for their co-performer in one of the following ways:
    - ID and liveness (biometric) test per above, plus signed consent form upload. Our internal moderators review the result of the ID and liveness, and the terms of the consent form.
    - Upload a photo and ID plus signed consent form. ID is validated by a third party ID validation service, with our internal moderators verifying the result of the ID validation, that the face of the co-performer matches the ID, and the terms of the consent form.
    - ID and Release form package. Upload copies of photo, ID, and signed consent form which is then reviewed by our internal moderators, verifying the face of the co-performer matches the ID and the terms of the consent form.
    - eSign (provided by Yoti). Co-performer undergoes ID, liveness (biometric) and performs e-signature of consent form. If co-performer ID has been uploaded separately previously, this option also supports reduced steps, with just the liveness and e-signature.
    - Existing content creator. Where two or more registered and verified content creators feature in the same content, they are able to tag each other, requiring affirmative consent.
- All co-performers must be approved by a member of our internal moderation team. All performers appearing in uploaded content are checked by the moderators against approved co-performers, to ensure everyone appearing in content uploaded by content creators can be matched to an ID-verified and approved co-performer. If there is any doubt, then further documentation will be requested from the uploader before the content is published. For example, if the content does not feature a face that can be compared to the identity documents, then further images may be required to ascertain that they are the same person. Ensuring identity and age of performers are verified and validated before publication severely limits the risk of potentially illegal material from upload.
- Note, some older content on the platform fell under an older policy where the content creator was required to attest to having ID and consent records for co-performers but before the company began validating either one or both requirements for all content prior to publication. However, per the timeline near the beginning of this document, we have announced a 30 June 2025 deadline

for individual verified uploaders to submit ID and consent paperwork for all co-performers in previously uploaded content. Older videos that do not meet our current verification requirements will be removed from the platform by that date. For details, see our blog post.: https://www.pornhub.com/blog/2025-consent-and-id-requirement-updates.

- Content partners must first go through an on-boarding process (see **Annex 1 – CPP Onboarding Process v1.2**).
- As it relates to content partners, studio-produced content follows record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content. While their website(s) and sample ID and consent paperwork are audited at onboarding and annually, they are not required to provide us with IDs for all performers prior to content publication. This part of the verification process is managed by the studios, and they are required to provide all documentation on demand:
    - Content partners are required to go through a KYC process to validate their identity and business. (see **Annex 2 - KYC Process V1.1**)
    - All content partners go through an annual audit where they are required to provide documentation for a random selection of their content.
- Further information on the verification process can be found in the following documentation:
    - How to Sign Up and Join the Model Program – Pornhub Help, including the video tutorial on this page
    - Yoti Tech documentation: Overview - Yoti developer documentation
    - Yoti Demo: Yoti Identity verification
- We have also now added INCODE as an additional identity verification provider.
- This robust and comprehensive process deters and helps to mitigate the risks relating to potential uploads of illegal material and to the potential commission of illegal acts on the platform.

Software tools are in place to detect known CSAM before publication

- PhotoDNA scans all images and YouTube CSAI Match scans all videos against hash-lists of known CSAM from the following organisations:
    - The Internet Watch Foundation: Image Hash List - Image Hash List (iwf.org.uk)
    - Thorn: Safer - How CSAM Detection Works | Safer by Thorn
    - National Center for Missing and Exploited Children: Hash sharing - CyberTipline Data (missingkids.org) and Take it Down - Take It Down (ncmec.org)
    - Offlimits: Instant Image Identifier - Offlimits | Home
    - Aylo's own hash databases from Mediawise and Safeguard
- PhotoDNA uses perceptual hashing techniques to scan uploaded content for matches against known CSAM hash-lists – PhotoDNA | Microsoft.

- Matches prevent the content from being published. This reduces the risk of CSAM from being published on the platform.

Software tools are in place to assist in the detection of unknown CSAM before publication

- All images and videos are scanned using three similar tools to help detect underage material:
    - Google Content Safety API: Developing and sharing tools to fight child sexual abuse (protectingchildren.google) and in particular the testimonial from NCMEC
    - Thorn's Safer: How CSAM Detection Works | Safer by Thorn
    - Aylo's Age Estimation: We use a detection model to output an age score estimating the performers age.
- Each piece of software scans faces within uploads to ascertain whether a performer appears to be underage. Results of these scans are passed to human moderators to aid moderation of content uploads before publication. Different tools are used as, whilst similar, they function in different ways. This ensures a threefold check on all uploaded material. If tools believe a performer is underage then human moderators are alerted and will further scrutinise the material to aid in publication decisions. This drastically reduces the risk of CSAM being published on Pornhub.

Human moderation

- All images and videos are reviewed by at least one human moderator before being published on Pornhub. Human moderators check that the IDs provided by uploaders and performers match those within the material. If there are any concerns, then the moderator will reach out to the uploader to supply more information and documentation. Human moderators use the results from all tools to assist them in assessing the content and only publish material once they are confident that the material meets all of our policies and guidelines. Requiring moderation of all images and videos before publication, severely limits the likelihood of CSAM appearing on the platform.

Downloads are not permitted

- Downloads of content are not permitted on Pornhub and no download functionality is made available. This reduces the risk of content being downloaded and re-distributed on other platforms after takedown, reducing the harms associated with re-victimisation.

Fingerprinting illegal material

- All potential CSAM that has been flagged by moderators, either during the upload process, or subsequently removed, is fingerprinted (hashed) using two pieces of software:
    - Mediawise by Vobile – This is based on third-party MD5 flat file hashing.
    - Safeguard by Aylo – This is based on first-party perceptual hashing which can detect manipulated media which may appear different to the original upload. For example if material is edited in length, has changed in colouring or added watermarks, the material is still detected as the same media and prevented from being re-uploaded.

- These fingerprints are scanned before publication. This reduces the risk of previously identified CSAM from being re-uploaded to the platform.

Banned Words List

- The platform utilises a database of banned words and phrases, which are prevented from being entered into all user-input fields, including titles, descriptions, tags, playlists, and searches. The database contains words and terms from multiple sources, including NGOs, law enforcement, and the platform's own. See for example the IWF Keyword List – Keywords List (iwf.org.uk). Preventing the use of terms associated with CSAM reduces the risk of CSAM publication.

Deterrence messaging

- Searches for words and phrases associated with CSAM and within the platform's database, result in a CSAM deterrence message being shown and no results surfaced. A global deterrence message is provided by The Lucy Faithfull Foundation in the United Kingdom, and many jurisdiction specific messages are displayed, as provided by local NGOs who specialise in child protection and potential offender behaviour. Deterrence messages direct those who seek for CSAM terms within the platforms database, to seek help from the relevant NGO partner. Deterrence messages also starkly inform the user that what they are searching is illegal, children will have been harmed in its creation, and it cannot be found on the platform. Deterrence messaging not only prevents users from searching for CSAM material, but also informs, educates, and provides help to those who are searching. Reducing the risk of users wishing to consume such material in the first place. The successful effects of deterrence messaging are explored in this paper by the Lucy Faithfull Foundation, which also makes express reference to the use of this safeguard on Pornhub.
- [redacted]

Chatbot

- In partnership with the Internet Watch Foundation and the Lucy Faithfull Foundation, we launched a chatbot on Pornhub in the UK as their exclusive pilot partner in March 2022. The chatbot seeks to engage with adult pornography users attempting to search for sexual imagery of children. The results from the pilot were evaluated by the University of Tasmania and showed success.

Contextual Text Moderation

- Users can comment underneath videos presented on the platform. These comments are moderated using third-party software from Spectrum Labs AI. The software scans comments in a contextual manner, for multiple bad behaviours including the discussion of CSAM. Any volitive

comments are automatically removed from the site. This further reduces the likelihood of CSAM material, even in written form, from appearing on the platform.

De-listing of URLs from search results

- If CSAM material is subsequently removed from the platform then the URL is provided to search engines to de-list the link and prevent the material (whilst already removed) from appearing in search results of search engines.

Trusted Flagger Program

- Pornhub operates a trusted flagger program comprising 66 members who specialise in the removal of CSAM and Non-consensual content (NCC) from the internet. Most are NGOs who receive communications directly from members of the public to report content of themselves or others, that they believe is CSAM or NCC. Some law enforcement entities and government agencies are also part of the trusted flagger program.
- Trusted flaggers can report content for removal directly to the platform and all content reported in this manner is immediately and automatically de-published from the platform, then subsequently reviewed. The program ensures that NGOs can very quickly remove content, therefore reducing the risk of viewing by users of the platform, and limiting the harm to victims.

Content Removal Request

- A content removal request form (**CRR**) is linked at the bottom of every page on the platform. Content reported in this manner is immediately and automatically removed, once the reporter has confirmed their email address. This reduces the risk of viewing material and limits harm to victims.
- The platform also offers an anonymous CSAM reporting form where an email address is not required. Material reported in this manner is reviewed within just a few hours and de-published if it is found to violate our CSAM policy.

Content Flagging

- The platform offers another way for logged-in users to flag all images, videos, comments, and users. Content flagged in this manner will be reviewed by a moderator within just a few hours and de-published if it is found to violate our CSAM policy. This reduces the risk of viewing material and limits harm to victims.

User Profiles and Comments

- Profile pictures are treated as uploaded images, per our moderation process and are therefore moderated via tools and humans to ensure they do not breach our Terms of Service.
- Usernames are scanned using our Banned Words List (see below) to reduce the likelihood of terms associated with minors or CSAM being used.
- Whilst we permit anonymous user profiles, users cannot post images or videos prior to an identity verification as referenced above. Therefore, our mitigation measures severely limit the likelihood that users share CSAM.

- Our Banned Words List and Contextual Text Moderation also act on comments posted by all registered users.

Messaging

- The platform does not allow unregistered users to message anyone else on the platform.
- The platform does not allow registered users to message other users, only content creators.
- The platform does not allow images, videos or attachments to be sent through the messaging system.
- All users can be reported using the in-built functionality of the site.
- These policies and the raft of mitigation measures for all content severely limit the likelihood that CSAM or CSAM URLs are communicated via messages on the platform.

Non-consensual content (NCC) – Acts, Recordings, Distribution, and Manipulation

Severity The amount and extent of negative impact if a risk materializes	**Marginal – Critical**
	Affected viewers: Viewers are affected in different ways depending upon the type of non-consensual content: • Non-consensual acts: Viewers are likely to be affected due to the nature of the material (e.g. rape) – Critical • Non-consensual recordings: Viewers can be affected, but it may not be obvious that there is no consent to filming (e.g. hidden cameras, which could be faked as hidden) – Marginal – Critical • Non-consensual distribution (e.g. revenge porn/non-consensual intimate images/image-based sexual abuse) – Viewers are unlikely to be affected if they are not aware that those within the content have not consented to its distribution – Marginal • Non-consensual manipulation (e.g. deepfakes) – Viewers are more likely affected if they are aware of the individuals being subjected to deepfakes – Critical
	Affected victims: Victims of all types of NCC are likely to be highly affected by the distribution of the material – Critical
	Irreversibility of the damage: Removal can remedy, but will not remove the negative impact on those who saw it or those depicted in the content – Critical
Probability The likelihood of the risk materializing	**Remote**
	As our most recent transparency report shows, only a very small share of uploads contain NCC and an even smaller share of those uploads were removed after publication, and thus reached an audience on the platform. *"Of videos both uploaded and removed for violating our NCC policy in 2024 from July through December, which represents 0.04% of videos uploaded during this time, over 81% were removed before being viewed."* *"Videos uploaded in the last six months of 2024 and removed for violating our NCC policy accounted for 0.003% of total views of all videos uploaded in the second half of 2024."*

	Whilst the mitigation measures we have in place make it unlikely that the platform will be used to commission or facilitate the distribution of NCC, it remains a risk that bad actors could attempt this. However, as supported by the statistics in our transparency report, referenced above, the likelihood of success for bad actors is low. – Remote
Overall assessment	**Medium**

Mitigating measures in place

Identity and consent

There are two types of uploaders on Pornhub: individual content creators, often referred to as "Models", and content partners, or third-party professional content studios.

As part of their registration process, content partners are required to provide a company name, company/studio content website, and physical address or URL indicating the coordinates of their custodian of 2257 records (pursuant to the record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content).

Every new uploader is required to undergo identity verification with a third-party identity verification provider, which requires them to:

- Submit a government-issued ID, which is authenticated by the provider.
- Conduct a liveness test to ensure the users likeness matches the government-issued ID and they are one and the same person.
- The liveness test also ensures that the person is alive and real, not AI, not pre-recorded, not a still image.

At time of signup, and again at the time of each upload, all uploaders are required to attest that they have obtained and retained ID and consent to record and distribute content from all other performers appearing in their content.

As part of Pornhub's more extensive verification processes, for individual content creators these requirements are validated at least once per additional performer:

- Uploaders may meet the ID and consent verification requirement for their co-performer in one of the following ways:
    - ID and liveness (biometric) test per above, plus signed consent form upload. Our internal moderators review the result of the ID and liveness, and the terms of the consent form.
    - Upload a photo and ID plus signed consent form. ID is validated by a third party ID validation service, with our internal moderators verifying the result of the ID validation, that the face of the co-performer matches the ID, and the terms of the consent form.

- ID and Release form package. Upload copies of photo, ID, and signed consent form which is then reviewed by our internal moderators, verifying the face of the co-performer matches the ID and the terms of the consent form.
- eSign (provided by Yoti). Co-performer undergoes ID, liveness (biometric) and performs e-signature of consent form. If co-performer ID has been uploaded separately previously, this option also supports reduced steps, with just the liveness and e-signature.
- Existing content creator. Where two or more registered and verified content creators feature in the same content, they are able to tag each other, requiring affirmative consent.

- All co-performers must be approved by a member of our moderation team. All performers appearing in uploaded content are checked by the moderators against approved co-performers, to ensure everyone appearing in content uploaded by content creators can be matched to an ID-verified and approved co-performer . If there is any doubt then further documentation will be requested from the uploader before the content is published. For example, if the content does not feature a face that can be compared to the identity documents, then further images may be required to ascertain that they are the same person. Ensuring identity and age of performers are verified and validated before publication severely limits the risk of potentially illegal material from upload.
- Note, some older content on the platform fell under an older policy where the content creator was required to attest to having ID and consent records for co-performers but before the company began validating either one or both requirements for all content prior to publication. However, per the timeline near the beginning of this document, we have announced a 30 June 2025 deadline for individual verified uploaders to submit ID and consent paperwork for all co-performers in previously uploaded content. Older videos that do not meet our current verification requirements will be removed from the platform by that date. For details, see our blog post.
- Content partners must first go through an on-boarding process (see Annex 1 – CPP Onboarding Process v1.2).
- As it relates to content partners, studio-produced content follows record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content. While their website(s) and sample ID and consent paperwork are audited at onboarding and annually they are not required to provide us with IDs for all performers prior to content publication. This part of the verification process is managed by the studios, and they are required to provide all documentation on demand:
  - Content partners are required to go through a KYC process to validate their identity and business. (see **Annex 2 - KYC Process V1.1**)
  - All content partners go through an annual audit where they are required to provide documentation for a random selection of their content.
- Further information on the verification process can be found in the following documentation:
  - How to Sign Up and Join the Model Program – Pornhub Help, including the video tutorial on this page
  - Yoti Tech documentation: Overview - Yoti developer documentation

- Yoti Demo: Yoti Identity verification

- We have also now added INCODE as an additional identity verification provider.
- This robust process deters and helps to mitigate the risk relating to the upload of illegal material, or committing any illegal acts on the platform.

Withdrawal of consent

- Performers who previously consented to the distribution of content on the platform can withdraw their consent at any time. This will result in the content being removed from the platform and can be reported via the CRR or by contacting our support team.

Software tools are in place to detect known non-consensual intimate images (NCII) before publication

- PhotoDNA scans all images, and YouTube CSAI Match scans all videos, against hash-lists of known NCII from the following organisation:
  - STOPNCII.org (part of the Revenge Porn Helpline)
- Matches prevent the content from being published. This reduces the risk of NCII from being published on the platform.

Human moderation

- All images and videos are reviewed by at least one human moderator before being published on the platform. Human moderators check that the IDs provided by uploaders and performers match those within the material. If there are any concerns, then the moderator will reach out to the uploader to supply more information and documentation. Human moderators use the results from all tools to assist them in assessing the content and only publish material once they are confident that the material meets all of our policies and guidelines. Requiring moderation of all images and videos before publication, severely limits the likelihood of NCC appearing on the platform.

Downloads are not permitted

- Downloads of content are not permitted on Pornhub, and no download functionality is made available. This reduces the risk of content being downloaded and re-distributed on other platforms even after takedown from Pornhub, reducing the harms associated with re-victimisation.

Fingerprinting illegal material

- All NCC that has been flagged by moderators, either during the upload process, or subsequently removed, is fingerprinted (hashed) using two pieces of software:
  - Mediawise by Vobile – This is based on third-party MD5 flat file hashing.
  - Safeguard by Aylo – This is based on first-party perceptual hashing which can detect manipulated media which may appear different to the original upload. For example if

material is edited in length, has been changed in colouring, or has added watermarks, the material is still detected as the same media and prevented from being re-uploaded.

- These fingerprints are scanned before publication. This reduces the risk of previously identified NCC from being re-uploaded to the platform.

Banned Words List

- The platform utilises a database of banned words and phrases, which are prevented from being entered into all user-input fields, including titles, descriptions, tags, playlists, and searches. The database contains words and terms from multiple sources, including NGOs, law enforcement, and the platforms own. Preventing the use of terms associated with all categories of NCC reduces the risk of NCC publication.

Deterrence messaging

- Searches for words and phrases associated with NCC and within the platform's database, result in an NCC deterrence message being shown and no results surfaced. A global deterrence message is provided by the Cyber Civil Rights Initiative in the United States of America, and many jurisdiction specific messages are displayed, as provided by local NGOs who specialise in NCC removal and victim support. Deterrence messages inform the user that what they are searching for is illegal and it cannot be found on the platform. Users are directed to NGOs who can help them if they are the victim of such material, and how to remove it if it appears on the platform or on other sites, via NGO resources. Deterrence messaging not only prevents users from searching for NCC material, but also informs, educates, and provides help to those who are searching. Reducing the risk of users wishing to consume such material in the first place.

Contextual Text Moderation

- Users can comment underneath videos presented on the platform. These comments are moderated using third-party software from Spectrum Labs AI. The software scans comments in a contextual manner, for multiple bad behaviours including the discussion of NCC. Any volitive comments are automatically removed from the site. This further reduces the likelihood of NCC material, even in written form, from appearing on the platform.

De-listing of URLs from search results

- If NCC material is subsequently removed from the platform then the URL is provided to search engines to de-list the link and prevent the material (whilst already removed) from appearing in search results of search engines.

Trusted Flagger Program

- Pornhub operates a trusted flagger program comprising 66 members who specialise in the removal of CSAM and NCII from the internet. Most are NGOs who receive communications directly from members of the public to report content of themselves or others, that they believe is CSAM or NCII. Some law enforcement entities and government agencies are also part of the trusted flagger program.

- Trusted flaggers can report content for removal directly to the platform and all content reported in this manner is immediately and automatically de-published from the platform, then subsequently reviewed. The program ensures that NGOs can very quickly remove content, therefore reducing the risk of viewing by users of the platform, and limiting the harm to victims.
- [redacted]

Content Removal Request

- A content removal request form (**CRR**) is linked at the bottom of every page on the platform. All visitors to the platform can use the CRR to report NCC material by providing the URL of the content, the reason why it should be removed, and an email address so that the platform can communicate with the reporter, ask for more detail if required, and confirm our decision. Content reported in this manner is immediately and automatically removed, once the reporter has confirmed their email address. This reduces the risk of viewing material and limits harm to victims.

Content Flagging

- The platform offers another way for logged-in users to flag all images, videos, comments, and users. Content flagged in this manner will be reviewed by a moderator within just a few hours and de-published if it is found to violate our NCC policy. This reduces the risk of viewing material and limits harm to victims.

Image-based Sexual Abuse Principles

- After the White House issued a Call to Action to Combat Image-Based Sexual Abuse for tech and civil society on 23 May 2024, the Center for Democracy and Technology (CDT), the Cyber Civil Rights Initiative (CCRI), and the National Network to End Domestic Violence (NNEDV) invited civil society organizations and tech industry leaders to a multistakeholder working group ("Working Group") focused on combating Image-Based Sexual Abuse.
- Aylo participated in this working group, which worked to create a set of principles, which were published in September 2024. We are proud of our continued work to prevent non-consensual content and hope that more organisations will sign-up to these voluntary principles.

Doxing and harassment

Severity The amount and extent of negative impact if a risk materializes	**Marginal – Critical**
	Affected viewers: The harm to users through seeing harassment is limited, unless they know the victim, which is unlikely. Doxing on the platform can make users feel uneasy that the platform is not safe – Marginal
	Affected victims: Harm to victims of doxing/harassment could be severe depending upon the nature of the threats and the personally identifiable information (PII) revealed. However, performers typically understand the inherent risk associated with appearing in adult content on an online platform – Marginal – Critical
	Irreversibility of the damage: Removal can help remedy, but will not remove the negative impact on the victims – Critical
Probability The likelihood of the risk materializing	**Remote – Occasional**
	Due to mitigating factors, harassment, stalking, and threats of abuse with critical impact only has a remote likelihood. Our platform does not facilitate such behaviour in a way that a other platforms may, for example, user to user messaging is not possible, user to content creator messaging is restricted, and we do not use location sharing functions. That said, there is a higher risk to content creators, and we therefore take their welfare seriously as shown in the mitigation measures below – Remote
Overall assessment	**Medium**

Mitigating measures in place

Resources for performers

- Guidelines are given to performers to help them understand how to protect their identity. This includes:
    - Educational blog posts with best practices for safety and security measures are published frequently, including:

https://www.pornhub.com/blog/increased-security-for-your-pornhub-account, https://www.pornhub.com/blog/tips-on-how-to-manage-account-security-and-safety and https://www.pornhub.com/blog/beware-of-phishing-scams-targeting-models

  - Monthly newsletters are circulated when new security features become available on the platform
  - Campaigns with 3rd party performer advocacy groups are in the works to share tips and knowledge on how performers can protect their address and other PII when filming content in their home – Cupcake Girls and Pornhub Announce New Partnership
  - Pornhub 101 series published for both users and models explain compliance and community elements of the platform

- We are working with third party advocacy groups via our partnerships to create assets to help our community better understand these as well.

Identity and consent

There are two types of uploaders on Pornhub: individual content creators, often referred to as "Models", and content partners, or third-party professional content studios.

As part of their registration, content partners are required to provide a company name, company/studio content website, and physical address or URL indicating the coordinates of their custodian of 2257 records (pursuant to record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content).

Every new uploader is required to undergo identity verification with a third-party identity verification provider, which requires them to:

- Submit a government issued ID, which is authenticated by the provider.
- Conduct a liveness test to ensure the users likeness matches the government issued ID and they are one and the same person.
- The liveness test also ensures that the person is alive and real, not AI, not pre-recorded, not a still image.

At time of signup, and again at the time of each upload, all uploaders are required to attest that they have obtained and retained ID and consent to record and distribute content from all other performers appearing in their content.

As part of Pornhub's more extensive verification processes, for individual content creators, these requirements are validated at least once per additional performer:

- Uploaders may meet the ID and consent verification requirement for their Co-performer in one of the following ways:
  - ID and liveness (biometric) test per above, plus signed consent form upload. Our moderators review the result of the ID and liveness, and the terms of the consent form.

- Upload a photo and ID plus signed consent form. ID is validated by a third party ID validation service, with our moderators verifying the result of the ID validation, that the face of the co-performer matches the ID, and the terms of the consent form.
- ID and Release form package. Upload copies of photo, ID, and signed consent form which is then reviewed by internal moderators, verifying the face of the co-performer matches the ID and the terms of the consent form.
- eSign (provided by Yoti). Co-performer undergoes ID, liveness (biometric) and performs e-signature of consent form. If co-performer ID has been uploaded separately previously, this option also supports reduced steps, with just the liveness and e-signature.
- Existing content creator. Where two or more registered and verified content creators feature in the same content, they are able to tag each other, requiring affirmative consent.

- All co-performers must be approved by a member of the moderation team. All performers appearing in uploaded content are checked by moderators against approved co-performers, to ensure everyone appearing in content uploaded by content creators can be matched to an ID-verified and approved co-performer . If there is any doubt then further documentation will be requested from the uploader before the content is published. For example, if the content does not feature a face that can be compared to the identity documents, then further images may be required to ascertain that they are the same person. Ensuring identity and age of performers are verified and validated before publication severely limits the risk of potentially illegal material from upload.
- Note, some older content on the platform fell under an older policy where the content creator was required to attest to having ID and consent records for co-performers but before the company began validating either one or both requirements for all content prior to publication. However, per the timeline near the beginning of this document, we have announced a 30 June 2025 deadline for individual verified uploaders to submit ID and consent paperwork for co-performers in previously uploaded content. Older videos that do not meet our current verification requirements will be removed from the platform by that date. For details, see our blog post.
- Content partners must first go through an on-boarding process (see Annex 1 – CPP Onboarding Process v1.2).
- As it relates to content partners, Studio produced content follows record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content.. While their website(s) and sample ID and consent paperwork are audited at onboarding and annually they are not required to provide us with IDs for all performers prior to content publication. This part of the verification process is managed by the studios, and they are required to provide all documentation on demand:
    - Content partners are required to go through a KYC process to validate their identity and business. (see **Annex 2 - KYC Process V1.1**)
    - All content partners go through an annual audit where they are required to provide documentation for a random selection of their content.
- Further information on the verification process can be found in the following documentation:

- How to Sign Up and Join the Model Program – Pornhub Help, including the video tutorial on this page
- Yoti Tech documentation: Overview - Yoti developer documentation
- Yoti Demo: Yoti Identity verification

- We have also now added INCODE as an additional identity verification provider.
- This robust process deters and helps to mitigate the risk relating to the upload of illegal material, or committing any illegal acts on the platform.

User profiles

- The information displayed on user profiles is limited and set by the user themselves.
- Two-factor authentication is available to all content creators on the platform to limit the likelihood of unauthorised access.
- Usernames cannot be edited by a user. Content creators can change their username and stage name once per month without contacting a support agent.
- A user harassing a content creator is mitigated by the content creator's ability to report the user, who would be actioned by the support team.
- Content creators can also contact our support team directly if a pattern of bad behaviour occurs.

Fake User profiles

- Noted in the messaging section, user to user messaging is not possible on the platform, therefore limiting the risk of users being harassed or contacted by other users.

Contextual Text Moderation

- Users can comment underneath videos presented on the platform. These comments are moderated using third-party software from Spectrum Labs AI. The software scans comments in a contextual manner, for multiple bad behaviours including the discussion of PII. Any volitive comments are automatically removed from the site. This reduces the likelihood of PII/doxing/harassment appearing on the platform.

Content Flagging

- The platform offers a way for logged-in users to flag all images, videos, comments, and users. Content flagged in this manner will be reviewed by a moderator within just a few hours and de-published if it is found to contain PII or doxing/harassment. Performers can flag users for doxing and threats to the Model Support team. These are reported to the Trust & Safety team to determine if there is an imminent threat, and they will take who will take the appropriate action. In most cases, the user is banned for violating our Terms of Service. This reduces the risk of viewing material and limits harm to victims.

Messaging

- The platform does not allow unregistered users to message anyone else on the platform.
- The platform does not allow registered users to message other users, only content creators.
- The platform does not allow images, videos or attachments to be sent through the messaging system.
- All users can be reported using the in-built functionality of the site.

Copyright infringements

Severity The amount and extent of negative impact if a risk materializes	**Marginal**
	Affected users: Users are likely to be unaffected – Slight
	Rights holders: The severity of the risk depends upon the nature of the copyright material. • If material from a private site (e.g. Only Fans) is concerned, then violations are more harmful than distribution of professionally produced material. • If material from a Hollywood movie or professionally produced material is concerned, then the risk of harm is low.
	Irreversibility of the damage: Damage can be reversed in some regard as once the material has been removed, then the copyright ceases to be infringed. Removal can remedy to a high degree and restore the prior situation – Marginal
Probability The likelihood of the risk materializing	**Improbable**
	The risk is improbable due to mitigating factors.
Overall assessment	**Low**

Mitigating measures in place

Identity and consent

There are two types of uploaders on Pornhub: individual content creators, often referred to as "Models", and content partners, or third-party professional content studios.

As part of their registration, content partners are required to provide a company name, company/studio content website, and physical address or URL indicating the coordinates of their custodian of 2257 records (pursuant to record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content).

Every new uploader is required to undergo identity verification with a third-party identity verification provider, which requires them to:

- Submit a government issued ID, which is authenticated by the provider.
- Conduct a liveness test to ensure the users likeness matches the government issued ID and they are one and the same person.

- The liveness test also ensures that the person is alive and real, not AI, not pre-recorded, not a still image.

At time of signup, and again at the time of each upload, all uploaders are required to attest that they have obtained and retained ID and consent to record and distribute content from all other performers appearing in their content.
As part of Pornhub's more extensive verification processes, for individual content creators, these requirements are validated at least once per additional performer:

- Uploaders may meet the ID and consent verification requirement for their Co-performer in one of the following ways:
    - ID and liveness (biometric) test per above, plus signed consent form upload. Our moderators review the result of the ID and liveness, and the terms of the consent form.
    - Upload a photo and ID plus signed consent form. ID is validated by a third party ID validation service, with our moderators verifying the result of the ID validation, that the face of the co-performer matches the ID, and the terms of the consent form.
    - ID and Release form package. Upload copies of photo, ID, and signed consent form which is then reviewed by internal moderators, verifying the face of the co-performer matches the ID and the terms of the consent form.
    - eSign (provided by Yoti). Co-performer undergoes ID, liveness (biometric) and performs e-signature of consent form. If co-performer ID has been uploaded separately previously, this option also supports reduced steps, with just the liveness and e-signature.
    - Existing content creator. Where two or more registered and verified content creators feature in the same content, they are able to tag each other, requiring affirmative consent.
- All co-performers must be approved by a member of the moderation team. All performers appearing in uploaded content are checked by moderators against approved co-performers, to ensure everyone appearing in content uploaded by content creators can be matched to an ID-verified and approved co-performer . If there is any doubt then further documentation will be requested from the uploader before the content is published. For example, if the content does not feature a face that can be compared to the identity documents, then further images may be required to ascertain that they are the same person. Ensuring identity and age of performers are verified and validated before publication severely limits the risk of potentially illegal material from upload.
- Note, some older content on the platform fell under an older policy where the content creator was required to attest to having ID and consent records for co-performers but before the company began validating either one or both requirements for all content prior to publication. However, per the timeline near the beginning of this document, we have announced a 30 June 2025 deadline for individual verified uploaders to submit ID and consent paperwork for co-performers in previously uploaded content. Older videos that do not meet our current verification requirements will be removed from the platform by that date. For details, see our blog post.
- Content partners must first go through an on-boarding process (see Annex 1 – CPP Onboarding Process v1.2).

- As it relates to content partners, Studio produced content follows record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content.. While their website(s) and sample ID and consent paperwork are audited at onboarding and annually they are not required to provide us with IDs for all performers prior to content publication. This part of the verification process is managed by the studios, and they are required to provide all documentation on demand:
    - Content partners are required to go through a KYC process to validate their identity and business. (see **Annex 2 - KYC Process V1.1**)
    - All content partners go through an annual audit where they are required to provide documentation for a random selection of their content.
- Further information on the verification process can be found in the following documentation:
    - How to Sign Up and Join the Model Program – Pornhub Help, including the video tutorial on this page
    - Yoti Tech documentation: Overview - Yoti developer documentation
    - Yoti Demo: Yoti Identity verification
- We have also now added INCODE as an additional identity verification provider.
- This robust process deters and helps to mitigate the risk relating to the upload of illegal material, or committing any illegal acts on the platform.

Software tools are in place to detect known copyright material before publication

- There are two repositories of Vobile hashes:
    - Hashes of content which violates our terms of service
    - Copyright content hashes.
- Exclusive model content is automatically fingerprinted by Vobile in the latter repository. If that content is uploaded by a different model in the future, the content will automatically be set to infringing copyright status.

Human moderation

- All images and videos are reviewed by at least one human moderator before being published on the platform. Human moderators check that the IDs provided by uploaders and performers match those within the material. If there are any concerns, then the moderator will reach out to the uploader to supply more information and documentation. Human moderators use the results from all tools to assist them in assessing the content and only publish material once they are confident that the material meets all of our policies and guidelines. Requiring moderation of all images and videos before publication, severely limits the likelihood of copyright material appearing on the platform.

Downloads are not permitted

- Downloads of content are not permitted on the platform. This reduces the risk of content being downloaded and re-distributed on other platforms even after having been taken down on Pornhub.

Fingerprinting illegal material

- All copyright material (produces by exclusive models) that has been flagged by moderators, either during the upload process, or subsequently removed, is fingerprinted (hashed) using two pieces of software:
    - Mediawise by Vobile – This is based on third-party MD5 flat file hashing.
    - Safeguard by Aylo – This is based on first-party perceptual hashing which can detect manipulated media which may appear different to the original upload. For example if material is edited in length, has changed in colouring, or added watermarks, the material is still detected as the same media and prevented from being re-uploaded .
- These fingerprints are scanned before publication. This reduces the risk of previously identified copyright material from being re-uploaded to the platform.

Tailored Reporting Forms

- Pornhub has DSA compliant content removal forms to report copyright infringements (alongside any other form of illegal content). Additionally, we prevent and enforce against copyright infringements globally with tailored processed and forms that take special requirements of non-EU jurisdictions into account. Pornhub also has a dedicated page on DMCA removals linked at the bottom of every page on the platform. Rights holders can use the DMCA form to report copyright material by providing the URL of the content, a description of the work being infringed, and full contact details. Content reported in this manner is reviewed by the DMCA team and investigated for removal. This reduces the risk of copyright material and limits harm to victims globally.

Terrorism

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected viewers: Anyone who sees it. The reach depends upon how long the material remains on the site and the number of views – Critical
	Number of affected victims: The number of victims is very limited – Slight
	Irreversibility of the damage: Removal can remedy, but will not remove the negative impact on those who saw it or those within it – Critical
Probability The likelihood of the risk materializing	**Improbable**
	Also due to mitigating factors, it is rare that we receive uploads of terrorist material.
Overall assessment	**Medium**

Mitigating measures in place

Identity and consent

There are two types of uploaders on Pornhub: individual content creators, often referred to as "Models", and content partners, or third-party professional content studios.

As part of their registration, content partners are required to provide a company name, company/studio content website, and physical address or URL indicating the coordinates of their custodian of 2257 records (pursuant to record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content).

Every new uploader is required to undergo identity verification with a third-party identity verification provider, which requires them to:

- Submit a government issued ID, which is authenticated by the provider.
- Conduct a liveness test to ensure the users likeness matches the government issued ID and they are one and the same person.
- The liveness test also ensures that the person is alive and real, not AI, not pre-recorded, not a still image.

At time of signup, and again at the time of each upload, all uploaders are required to attest that they have obtained and retained ID and consent to record and distribute content from all other performers appearing in their content.

As part of Pornhub's more extensive verification processes, for individual content creators, these requirements are validated at least once per additional performer:

- Uploaders may meet the ID and consent verification requirement for their Co-performer in one of the following ways:
    - ID and liveness (biometric) test per above, plus signed consent form upload. Our moderators review the result of the ID and liveness, and the terms of the consent form.
    - Upload a photo and ID plus signed consent form. ID is validated by a third party ID validation service, with our moderators verifying the result of the ID validation, that the face of the co-performer matches the ID, and the terms of the consent form.
    - ID and Release form package. Upload copies of photo, ID, and signed consent form which is then reviewed by internal moderators, verifying the face of the co-performer matches the ID and the terms of the consent form.
    - eSign (provided by Yoti). Co-performer undergoes ID, liveness (biometric) and performs e-signature of consent form. If co-performer ID has been uploaded separately previously, this option also supports reduced steps, with just the liveness and e-signature.
    - Existing content creator. Where two or more registered and verified content creators feature in the same content, they are able to tag each other, requiring affirmative consent.
- All co-performers must be approved by a member of the moderation team. All performers appearing in uploaded content are checked by moderators against approved co-performers, to ensure everyone appearing in content uploaded by content creators can be matched to an ID-verified and approved co-performer . If there is any doubt then further documentation will be requested from the uploader before the content is published. For example, if the content does not feature a face that can be compared to the identity documents, then further images may be required to ascertain that they are the same person. Ensuring identity and age of performers are verified and validated before publication severely limits the risk of potentially illegal material from upload.
- Note, some older content on the platform fell under an older policy where the content creator was required to attest to having ID and consent records for co-performers but before the company began validating either one or both requirements for all content prior to publication. However, per the timeline near the beginning of this document, we have announced a 30 June 2025 deadline for individual verified uploaders to submit ID and consent paperwork for co-performers in previously uploaded content. Older videos that do not meet our current verification requirements will be removed from the platform by that date. For details, see our blog post.
- Content partners must first go through an on-boarding process (see Annex 1 – CPP Onboarding Process v1.2).
- As it relates to content partners, Studio produced content follows record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and

maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content.. While their website(s) and sample ID and consent paperwork are audited at onboarding and annually they are not required to provide us with IDs for all performers prior to content publication. This part of the verification process is managed by the studios, and they are required to provide all documentation on demand:

    - Content partners are required to go through a KYC process to validate their identity and business. (see **Annex 2 - KYC Process V1.1**)
    - All content partners go through an annual audit where they are required to provide documentation for a random selection of their content.

- Further information on the verification process can be found in the following documentation:
    - How to Sign Up and Join the Model Program – Pornhub Help, including the video tutorial on this page
    - Yoti Tech documentation: Overview - Yoti developer documentation
    - Yoti Demo: Yoti Identity verification
- We have also now added INCODE as an additional identity verification provider.
- This robust process deters and helps to mitigate the risk relating to the upload of illegal material, or committing any illegal acts on the platform.

Membership of Tech Against Terrorism

- PH is a member of Tech Against Terrorism's mentorship program – Tech Against Terrorism | Disrupting Terrorist Activity Online which mentors platforms in preventing the dissemination of terrorist material, giving access to threat intelligence, OSINT briefings, and a knowledge sharing platform.

Terrorist Content Online Regulation compliance

- We comply with the Terrorist Content Online Regulation in the EU, requiring immediate takedown of any material reported by the relevant authorities, as noted in our Terms of Service. *"For any removal orders pursuant to Regulation (EU) 2021/784 (the "Terrorist Content Online Regulation" or "TCO"), designated competent EU authorities can complete our removal form. After submission of this form, you will receive further instructions by e-mail, which you may respond to with a removal order. For such removal orders, please use the template provided in Annex I of the TCO and conduct all communication in either English or Greek."*

User Profiles

- Profile pictures are treated as uploaded images, per our moderation process and are therefore moderated via tools and humans to ensure they do not breach our Terms of Service.
- Usernames are scanned using our Banned Words List (see below) to reduce the likelihood of hateful terms being used.

- Usernames cannot be edited by a user. Content creators can change their username and stage name once per month without contacting a support agent.
- Whilst we permit anonymous user profiles, our mitigation measures severely limit the likelihood that users share terrorism material.

Human moderation

- All images and videos are reviewed by at least one human moderator before being published on the platform. Human moderators check that the IDs provided by uploaders and performers match those within the material. If there are any concerns, then the moderator will reach out to the uploader to supply more information and documentation. Human moderators use the results from all tools to assist them in assessing the content and only publish material once they are confident that the material meets all of our policies and guidelines. Requiring moderation of all images and videos before publication, severely limits the likelihood of terrorist content appearing on the platform.

Downloads are not permitted

- Downloads of content are not permitted on the platform. This reduces the risk of content being downloaded and re-distributed on other platforms even after takedown from Pornhub, reducing the harms associated with re-victimisation.

Fingerprinting illegal material

- All terrorist material that has been flagged by moderators, either during the upload process, or subsequently removed, is fingerprinted (hashed) using two pieces of software:
    - Mediawise by Vobile – This is based on third-party MD5 flat file hashing.
    - Safeguard by Aylo – This is based on first-party perceptual hashing which can detect manipulated media which may appear different to the original upload. For example if material is edited in length, has been changed in colouring, or has added watermarks, the material is still detected as the same media and prevented from being re-uploaded.
- These fingerprints are scanned before publication. This reduces the risk of previously identified terrorist content from being re-uploaded to the platform.

Banned Words List

- The platform utilises a database of banned words and phrases, which are prevented from being entered into all user-input fields, including titles, descriptions, tags, playlists, and searches. The database contains words and terms from multiple sources, including NGOs, law enforcement, and the platforms own. Preventing the use of terms associated with terrorism reduces the risk of terrorist material publication.

De-listing of URLs from search results

- If terrorist material is subsequently removed from the platform then the URL is provided to search engines to de-list the link and prevent the material (whilst already removed) from appearing in search results of search engines.

Content Removal Request

- A content removal request form (**CRR**) is linked at the bottom of every page on the platform. Content reported in this manner is immediately and automatically removed, once the reporter has confirmed their email address. This reduces the risk of viewing material and limits harm to victims.

Content Flagging

The platform offers another way for logged-in users to flag all images, videos, comments, and users. Content flagged in this manner will be reviewed by a moderator within just a few hours and de-published if it is found to violate our terms of service. This reduces the risk of terrorist material from being viewed.

Contextual Text Moderation

- Users can comment underneath content presented on the platform, including videos and blog posts. These comments are moderated using third-party software from Active Fence. The software scans comments in a contextual manner, for multiple bad behaviours including the discussion of violence. Any violative comments are reviewed and removed from the site.

Messaging

- The platform does not allow unregistered users to message anyone else on the platform.
- The platform does not allow registered users to message other users, only content creators.
- The platform does not allow images, videos or attachments to be sent through the messaging system.
- All users can be reported using the in-built functionality of the site.
- These measures limit the likelihood that terrorist material can be shared on our platform.

AI-generated content representing illegal acts

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected viewers: Anyone who sees it. The reach depends upon how long the material remains on the site and the number of views – Critical
	Number of affected victims: The number of victims, where their likeness is used in AI-generated material is likely to be low.
	Irreversibility of the damage: Removal can remedy, but will not remove the negative impact on those within it – Critical
Probability The likelihood of the risk materializing	**Improbable**
	The risk is improbable due to mitigating factors.
Overall assessment	**Medium**

Mitigating measures in place

Policies

- Our policies surrounding illegal material (e.g. CSAM, NCC) include the prohibition of any depictions of illegal material, even if AI-generated. Our risk assessment and mitigation measures for such content, therefore also apply in this context.

Reference to further measures

- Please see the risk assessments on dissemination of the relevant type of illegal material for more information. As we require ID and consent documentation from every uploader and performer, something that is obviously impossible to receive from those within AI generated material, the risk here is inherently low.

Fundamental rights

Hate speech and fostering stereotypes regarding sexual preferences and behaviour

No matter the ethnicity, sexual orientation, gender, ability, or body type, the Pornhub community welcomes all consenting adults to connect, upload and share original content, shame-free. Our platform is for exploration and discovery, and we do not permit any discriminatory abuse towards any user.

Our Core values are Consent, Freedom of Sexual Expression, Authenticity, Originality, and Diversity.

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected viewers: Anyone who sees it. The reach depends upon how long the material remains on the site and the number of views – Critical
	Number of affected victims: Those who are the target of hate speech are likely to be a minority – Marginal
	Irreversibility of the damage: Removal can remedy, but will not remove the negative impact on those within it – Critical
Probability The likelihood of the risk materializing	**Remote**
	As our most recent transparency report shows, only a very small number of pieces of content were removed for hate speech. *"From July through December, we removed 26 pieces of content (10 videos and 16 photos) for violating our hate speech and violent speech policy."* The mitigation measures we have in place significantly reduce the likelihood that the platform can be used in this manner – Remote
Overall assessment	**Medium**

Mitigating measures in place

Policies

- We define hate speech as any communication or material that promotes, calls for, supports, or advocates for the delegitimization, dehumanization, discrimination, segregation, detestation, or vilification of a person or group of persons by reason of the fact that they are identifiable on the basis of protected characteristics. At its most extreme, hate speech calls for, threatens, or promotes violence against people that are identifiable on the basis of protected characteristics. Both our Terms of Service, and our policy on hate speech prohibit any material featuring hate speech.

User Profiles

- Usernames are scanned using our Banned Words List (see below) to reduce the likelihood of hateful terms being used.
- Usernames cannot be edited by a user. Content creators can change their username and stage name once per month without contacting a support agent.
- Profile pictures are treated as uploaded images, per our moderation processes and are therefore moderated via tools and humans to ensure they do not breach our Terms of Service.
- Whilst we permit anonymous user profiles, our mitigation measures severely limit the likelihood that users share hateful material.

Banned Words List

- The platform utilises a database of banned words and phrases, which are prevented from being entered into any user-input fields, including titles, descriptions, tags, playlists, and searches. The database contains words and terms from multiple sources, including NGOs, Law Enforcement, and the platforms own.

Contextual Text Moderation

- Users can comment underneath videos presented on the platform. These comments are moderated using third-party software from Spectrum Labs AI. The software scans comments in a contextual manner, for multiple bad behaviours including hate speech. Any violative comments are automatically removed from the platform. This further reduces the likelihood of discriminating material, even in written form, from appearing on the platform.

Human moderation

- All images and videos are reviewed by at least one human moderator before being published on the platform. Human moderators use the results from all tools to assist them in assessing the content and only publish material once they are confident that the material meets all of our policies and guidelines. Requiring moderation of all images and videos before publication, severely limits the likelihood of discriminatory content appearing on the platform

Content Removal Request

- A content removal request form (**CRR**) is linked at the bottom of every page on the platform. All visitors to the platform can use the CRR to report material by providing the URL of the content, the reason why it should be removed, and an email address so that the platform can communicate

with the reporter, ask for more detail if required, and confirm our decision. Content reported in this manner is immediately and automatically removed, once the reporter has confirmed their email address. This reduces the risk of viewing material and limits harm to victims.

Content Flagging

- The platform offers another way for logged-in users to flag all images, videos, comments, and users. Content flagged in this manner will be reviewed by a moderator within just a few hours and de-published if it is found to violate our Terms of Service. This reduces the risk of viewing material and limits harm to victims.

Law enforcement portal

- We host a law enforcement portal so that law enforcement is able to quickly request information from the platform to assist with legal cases.

Messaging

- The platform does not allow unregistered users to message anyone else on the platform.
- The platform does not allow registered users to message other users, only content creators.
- The platform does not allow images, videos or attachments to be sent through the messaging system.
- All users can be reported using the in-built functionality of the site.
- These policies and mitigation measures lower the risk of messaging being used to facilitate the spread of hate.

Freedom of Sexual Expression

- When acted out by consenting adults in safe environments and adhering to our Terms of Service, desires, fetishes and fantasies are welcomed and supported on our platform. Pornography does not always represent sexual interactions and behaviours typical of everyday life, and can depict diverse fantasies and role-play by consenting amateurs and professionals.

Strengthening a resilient community

- Donating to BIPOC Adult Industry Collective for Black History Month: We donated to the BIPOC Adult Industry Collective, an organization offering resources, education, and support services to help fight racism in the adult entertainment industry. The organization pursues this mission through various programs and activities designed to help community members reach their goals and fulfil their potential.
- Celebrating Excellence Throughout Black History Month: Our team is committed to fighting the stigma associated with sex work year-round. This Black History Month, we're contributing to this goal by humanizing Performers and creating links of recognition and understanding with those outside the adult entertainment industry through a Black Model Spotlight Series!
- Demystifying LGBTQ+ Slang in the Adult Industry: There's a lot of information online about the gay community, however some of it is rather incomplete, and sometimes downright offensive. We hope to clear away some of the confusion and offer you a clear and detailed breakdown of some

of the terms commonly used by lesbian, gay, bisexual, transgender, queer, and pansexual groups.

Sex trafficking

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Users: Users are unlikely to be aware of whether an individual has been trafficked, but would be affected if they were made aware and had seen the content, this number is likely very small – Marginal
	Number of affected victims: The number of sex trafficking victims is likely low and their damage is high.
	Irreversibility of the damage: Removal can remedy as those who saw material featuring trafficked individuals would not normally be aware. Removal would not change the effect on victims – Critical
Probability The likelihood of the risk materializing	**Remote**
	We mitigate the likelihood of sex trafficking occurring on the platform in multiple different ways, this lowers the risk, but cannot eliminate it completely due to the risk occurring outside our platform. Mitigating trafficking on our platform is handled by layering available measures to reduce the risk. Due to our extensive mitigation measures, not least our identity verification, consent requirements, and human moderation component, the risk of the platform being used in this manner is remote.
Overall assessment	**Medium**

Mitigating measures in place

Policies

- Our Terms of Service prohibit any content that "in any way that promotes or facilitates prostitution, solicitation of prostitution, human trafficking, or sex trafficking".
- Our Community Guidelines state that any content that constitutes or promotes any form of human trafficking, including sex trafficking, is prohibited.

User Profiles

- Content creators may choose to add information to their profile, but we provide the resources listed below to help performers keep themselves and the identity safe. See for example, the resources for performers described below.

Resources for performers

- Guidelines are given to performers to help them understand how to protect their identity. This includes:
    - Educational blog posts with best practices for safety and security measures are published frequently, including:

      https://www.pornhub.com/blog/increased-security-for-your-pornhub-account, https://www.pornhub.com/blog/tips-on-how-to-manage-account-security-and-safety and https://www.pornhub.com/blog/beware-of-phishing-scams-targeting-models
    - Monthly newsletters are circulated when new security features become available on the platform
    - Campaigns with 3rd party performer advocacy groups are in the works to share tips and knowledge on how performers can protect their address and other PII when filming content in their home – Cupcake Girls and Pornhub Announce New Partnership
    - Pornhub 101 series published for both users and models explain compliance and community elements of the platform
- We are working with third party advocacy groups via our partnerships to create assets to help our community better understand these as well.

Identity and consent

There are two types of uploaders on Pornhub: individual content creators, often referred to as "Models", and content partners, or third-party professional content studios.

As part of their registration, content partners are required to provide a company name, company/studio content website, and physical address or URL indicating the coordinates of their custodian of 2257 records (pursuant to record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content).

Every new uploader is required to undergo identity verification with a third-party identity verification provider, which requires them to:

- Submit a government-issued ID, which is authenticated by the provider.
- Conduct a liveness test to ensure the users likeness matches the government-issued ID and they are one and the same person.
- The liveness test also ensures that the person is alive and real, not AI, not pre-recorded, not a still image.

At time of signup, and again at the time of each upload, all uploaders are required to attest that they have obtained and retained ID and consent to record and distribute content from all other performers appearing in their content.

As part of Pornhub's more extensive verification processes, for individual content creators, these requirements are validated at least once per additional performer:

- Uploaders may meet the ID and consent verification requirement for their co-performer in one of the following ways:
    - ID and liveness (biometric) test per above, plus signed consent form upload. Our internal moderators review the result of the ID and liveness, and the terms of the consent form.
    - Upload a photo and ID plus signed consent form. ID is validated by a third party ID validation service, with our internal moderators verifying the result of the ID validation, that the face of the co-performer matches the ID, and the terms of the consent form.
    - ID and Release form package. Upload copies of photo, ID, and signed consent form which is then reviewed by our internal moderators, verifying the face of the co-performer matches the ID and the terms of the consent form.
    - eSign (provided by Yoti). Co-performer undergoes ID, liveness (biometric) and performs e-signature of consent form. If co-performer ID has been uploaded separately previously, this option also supports reduced steps, with just the liveness and e-signature.
    - Existing content creator. Where two or more registered and verified content creators feature in the same content, they are able to tag each other, requiring affirmative consent.
- All co-performers must be approved by a member of our internal moderation team. All performers appearing in uploaded content are checked by the moderators against approved co-performers, to ensure everyone appearing in content uploaded by content creators can be matched to an ID-verified and approved co-performer. If there is any doubt then further documentation will be requested from the uploader before the content is published. For example, if the content does not feature a face that can be compared to the identity documents, then further images may be required to ascertain that they are the same person. Ensuring identity and age of performers are verified and validated before publication severely limits the risk of potentially illegal material from upload.
- Note, some older content on the platform fell under an older policy where the content creator was required to attest to having ID and consent records for co-performers but before the company began validating either one or both requirements for all content prior to publication. However, per the timeline near the beginning of this document, we have announced a 30 June 2025 deadline for individual verified uploaders to submit ID and consent paperwork for co-performers in previously uploaded content. Older videos that do not meet our current verification requirements will be removed from the platform by that date. For details, see our blog post.
- Content partners must first go through an on-boarding process (see **Annex 1 – CPP Onboarding Process v1.2**).
- As it relates to content partners, Studio produced content follows record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content.. While their website(s) and sample ID and consent paperwork are audited at onboarding and annually they are not required to provide us with IDs for all performers prior to content publication. This part of the verification process is managed by the studios, and they are required to provide all documentation on demand:

- Content partners are required to go through a KYC process to validate their identity and business. (see **Annex 2 - KYC Process V1.1)**
- All content partners go through an annual audit where they are required to provide documentation for a random selection of their content.

- Further information on the verification process can be found in the following documentation:
  - How to Sign Up and Join the Model Program – Pornhub Help, including the video tutorial on this page
  - Yoti Tech documentation: Overview - Yoti developer documentation
  - Yoti Demo: Yoti Identity verification
- We have also now added INCODE as an additional identity verification provider.
- This robust process deters and helps to mitigate the risk relating to the upload of illegal material, or committing any illegal acts on the platform.
- .

Withdrawal of consent

- Performers who previously consented to the distribution of content on the platform can withdraw their consent at any time. This will result in the content being removed from the platform and be reported via the CRR.

Beneficiary controls

- Only the ID verified, main account holder can receive payments from their account on the platform. When an account is held by a couple, the beneficiary can be either individual.

Banned Words List

- The platform utilises a database of banned words and phrases, which are prevented from being entered into all user-input fields, including titles, descriptions, tags, playlists, and searches. The database contains words and terms from multiple sources, including NGOs, law enforcement, and the platforms own.

Human moderation

- All uploaded images and videos are reviewed by at least one human moderator before being published on the platform. Human moderators check that the IDs provided by uploaders and performers match those within the material. If there are any concerns, then the moderator will reach out to the uploader to supply more information and documentation. Human moderators use the results from all tools to assist them in assessing the content and only publish material once they are confident that the material does not violate our policies and guidelines. Requiring moderation of all images and videos before publication, limits the likelihood of content featuring victims of trafficking occurring.

Content Removal Request

- A content removal request form (**CRR**) is linked at the bottom of every page on the platform. All visitors to the platform can use the CRR to report material by providing the URL of the content, the reason why it should be removed, and an email address so that the platform can communicate with the reporter, ask for more detail if required, and confirm our decision. Content reported in this manner is immediately and automatically removed, once the reporter has confirmed their email address. This reduces the risk of viewing material and limits harm to victims.

Content Flagging

- The platform offers another way for logged-in users to flag all images, videos, comments, and users. Content flagged in this manner will be reviewed by a moderator within just a few hours and de-published if it is found to violate our Terms of Service. This reduces the risk of viewing material and limits harm to victims.

Law enforcement portal

- We host a law enforcement portal so that law enforcement is able to quickly request information from the platform to assist with legal cases.

Messaging

- The platform does not allow unregistered users to message anyone else on the platform.
- The platform does not allow registered users to message other users, only content creators.
- The platform does not allow images, videos or attachments to be sent through the messaging system.
- All users can be reported using the in-built functionality of the site.
- All messaging is un-encrypted.

Partnership with the Cupcake Girls

- The Cupcake Girls are an organization that provides advocacy and referral services to consensual sex workers, as well as prevention and aftercare services to those affected by sex trafficking. By sharing resources – ranging from collective collaborations to data insights – and by engaging with sex workers, the goal is to support consensual sex workers and foster an environment where their safety and success is prioritized.
- We partnered with the Cupcake Girls in September 2023 to support consensual sex workers and foster an environment where their safety and success is prioritised.
- In March 2025, Aylo announced a first-of-its-kind trafficking prevention safety video series for adult performers.

Data minimization

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected user: The affect depends upon the type user and the data that is leaked • Content creators: The number of content creators is relatively low – Medium • Visitor: Minimal data is collected on a user and as account creation is not required, the number of effected users would be low.
	Irreversibility of the damage: The damage cannot be reversed – Critical
Probability The likelihood of the risk materializing	**Remote**
	The risk is remote due to mitigating factors.
Overall assessment	**Medium**

Mitigating measures in place

Policies

- Our privacy policy makes clear the data we collect and the legal basis for its collection.

Data protection impact assessment

- Our data protection impact assessment for our identity verification providers, Yoti and Incode, are included within the supporting documentation (**Annex 3 - Data Protection Impact Assessment - YOTI - June 2024, Annex 4 - Data Protection Impact Assessment - INCODE - Feb 2025**). The data are stored by the Trust and Safety department at Aylo. Access to the data is restricted to a selected few to prevent unlawful access. Penetration testing and security evaluation is performed to Trust and Safety Platform internally. Yoti and Incode are audited annually against the SOC2 Type 2 Security control standards and also maintains ISO 27001 certification.

Civic Discourse, electoral process and public security

Politically provocative content and adverts

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected viewers: Anyone who sees it. The reach depends upon how long the material remains on the site and the number of views – Critical
	Irreversibility of the damage: Removal can remedy, but will not remove the negative impact on those who saw it or those within it – Critical
Probability The likelihood of the risk materializing	**Improbable**
	The risk is improbable due to mitigating factors.
Overall assessment	**Medium**

Mitigating measures in place

Policies

- Our community guidelines prohibit the upload of content that may cause harm to individuals, specifically content which: "Constitutes hate speech or inflammatory content, including violent extremism or **political provocation**."

Identity and consent

There are two types of uploaders on Pornhub: individual content creators, often referred to as "Models", and content partners, or third-party professional content studios.

As part of their registration, content partners are required to provide a company name, company/studio content website, and physical address or URL indicating the coordinates of their custodian of 2257 records (pursuant to record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content).

Every new uploader is required to undergo identity verification with a third-party identity verification provider, which requires them to:

- Submit a government-issued ID, which is authenticated by the provider.

- Conduct a liveness test to ensure the users likeness matches the government-issued ID and they are one and the same person.
- The liveness test also ensures that the person is alive and real, not AI, not pre-recorded, not a still image.

At time of signup, and again at the time of each upload, all uploaders are required to attest that they have obtained and retained ID and consent to record and distribute content from all other performers appearing in their content.
As part of Pornhub's more extensive verification processes, for individual content creators, these requirements are validated at least once per additional performer:

- Uploaders may meet the ID and consent verification requirement for their co-performer in one of the following ways:
    - ID and liveness (biometric) test per above, plus signed consent form upload. Our internal moderators review the result of the ID and liveness, and the terms of the consent form.
    - Upload a photo and ID plus signed consent form. ID is validated by a third party ID validation service, with our internal moderators verifying the result of the ID validation, that the face of the co-performer matches the ID, and the terms of the consent form.
    - ID and Release form package. Upload copies of photo, ID, and signed consent form which is then reviewed by internal moderators, verifying the face of the co-performer matches the ID and the terms of the consent form.
    - eSign (provided by Yoti). Co-performer undergoes ID, liveness (biometric) and performs e-signature of consent form. If co-performer ID has been uploaded separately previously, this option also supports reduced steps, with just the liveness and e-signature.
    - Existing content creator. Where two or more registered and verified content creators feature in the same content, they are able to tag each other, requiring affirmative consent.
- All co-performers must be approved by a member of the moderation team. All performers appearing in uploaded content are checked by moderators against approved co-performers, to ensure everyone appearing in content uploaded by content creators can be matched to an ID-verified and approved co-performer. If there is any doubt then further documentation will be requested from the uploader before the content is published. For example, if the content does not feature a face that can be compared to the identity documents, then further images may be required to ascertain that they are the same person. Ensuring identity and age of performers are verified and validated before publication severely limits the risk of potentially illegal material from upload.
- Note, some older content on the platform fell under an older policy where the content creator was required to attest to having ID and consent records for co-performers but before the company began validating either one or both requirements for all content prior to publication. However, per the timeline near the beginning of this document, we have announced a 30 June 2025 deadline for individual verified uploaders to submit ID and consent paperwork for co-performers in previously uploaded content. Older videos that do not meet our current verification requirements will be removed from the platform by that date. For details, see our blog post.

- Content partners must first go through an on-boarding process (see **Annex 1 – CPP Onboarding Process v1.2**).
- As it relates to content partners, Studio produced content follows record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content.. While their website(s) and sample ID and consent paperwork are audited at onboarding and annually they are not required to provide us with IDs for all performers prior to content publication. This part of the verification process is managed by the studios, and they are required to provide all documentation on demand:
    - Content partners are required to go through a KYC process to validate their identity and business. (see **Annex 2 - KYC Process V1.1**)
    - All content partners go through an annual audit where they are required to provide documentation for a random selection of their content.
- Further information on the verification process can be found in the following documentation:
    - How to Sign Up and Join the Model Program – Pornhub Help, including the video tutorial on this page
    - Yoti Tech documentation: Overview - Yoti developer documentation
    - Yoti Demo: Yoti Identity verification
- We have also now added INCODE as an additional identity verification provider.
- This robust process deters and helps to mitigate the risk relating to the upload of illegal material, or committing any illegal acts on the platform.

User Profiles

- User profiles on the platform show a limited amount of information which can be set by the user. The nature of our platform is such that it is unlikely to be targeted by those who wish to engage in foreign interference by targeting users via their profiles.
- Profile pictures are treated as uploaded images, per our moderation process and are therefore moderated via tools and humans to ensure they do not breach our Terms of Service.
- Anonymous users cannot post images and videos.
- Whilst we permit anonymous user profiles, our mitigation measures severely limit the likelihood that users share foreign interference information.

Fake User profiles

- Noted in the messaging section, user to user messaging is not possible on the platform, therefore limiting the risk of users being exploited by other users.
- Authoritative and high-profile sources are highly unlikely to create profiles on the platform due to the type of platform, nor would users expect this to the case, therefore limiting the likelihood that users would take anyone impersonating such a source, seriously.

- A user messaging a content creator is mitigated by the content creator's ability to report the user, who would be actioned by the support team.
- Content creators can also contact our support team directly if a pattern of bad behaviour occurs.

Contextual Text Moderation

- Users can comment underneath content presented on the platform, including videos and blog posts. These comments are moderated using third-party software from Active Fence. The software scans comments in a contextual manner, for multiple bad behaviours, including spam and associated URLs, hyperlinking in this regard would fall into. Any violative comments are reviewed and removed from the platform.

Human moderation

- All uploaded images and videos are reviewed by at least one human moderator before being published on the platform. Human moderators check that the IDs provided by uploaders and performers match those within the material. If there are any concerns, then the moderator will reach out to the uploader to supply more information and documentation. Human moderators use the results from all tools to assist them in assessing the content and only publish material once they are confident that the material does not violate our policies and guidelines. Requiring moderation of all images and videos before publication, severely limits the likelihood of any risk to civic discourse, electoral process and public security.

Downloads are not permitted

- Downloads of content are not permitted on the platform, and no download functionality is made available. This reduces the risk of content being downloaded and re-distributed on other platforms.

Fingerprinting illegal material

- All potential politically proactive content that has been flagged by moderators, either during the upload process, or subsequently removed, is fingerprinted (hashed) using two pieces of software:
    - Mediawise by Vobile – This is based on third-party MD5 flat file hashing.
    - Safeguard by Aylo – This is based on first-party perceptual hashing which can detect manipulated media which may appear different to the original upload. For example if material is edited in length, has changed in colouring, or added watermarks, the material is still detected as the same media and prevented from being re-uploaded.
- These fingerprints are scanned before publication. This reduces the risk of previously identified politically provocative content from being re-uploaded to the platform.

De-listing of URLs from search results

- If politically provocative material is subsequently removed from the platform then the URL is provided to search engines to de-list the link and prevent the material (whilst already removed) from appearing in search results of search engines.

Content Removal Request

- A content removal request form (**CRR**) is linked at the bottom of every page on the platform. Content reported in this manner is immediately and automatically removed, once the reporter has confirmed their email address. This reduces the risk of viewing material and limits harm to victims.

Content Flagging

- The platform offers another way for logged-in users to flag all images, videos, comments, and users. Content flagged in this manner will be reviewed by a moderator within just a few hours and de-published if it is found to violate our policies. This reduces the risk of viewing material and limits harm to victims.

Law enforcement portal

- We host a law enforcement portal so that law enforcement is able to quickly request information from the platform to assist with legal cases.

Messaging

- The platform does not allow unregistered users to message anyone else on the platform.
- The platform does not allow registered users to message other users, only content creators.
- The platform does not allow images, videos or attachments to be sent through the messaging system.
- All users can be reported using the in-built functionality of the site.
- All messaging is un-encrypted.

Deep fakes

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected viewers: Anyone who sees it. The reach depends upon how long the material remains on the site and the number of views – Critical
	Number of affected victims: Those who are the target of hate speech are likely to be a minority – Marginal
	Irreversibility of the damage: Removal can remedy, but will not remove the negative impact on those within it – Critical
Probability The likelihood of the risk materializing	**Improbable**
	The risk is improbable due to mitigating factors.
Overall assessment	**Medium**

Mitigating measures in place

Policies

- Our policies surrounding the dissemination of NCC, include non-consensually manipulated content (deep fakes). Our risk assessment and mitigation measures for such content, therefore also apply in this context.

Reference to further measures

- Please see the risk assessments on dissemination of NCC for more information. As we require ID and consent documentation from every uploader and performer, something that is obviously impossible to receive from those within deep fakes, the risk here is inherently low.

Over-blocking

Severity The amount and extent of negative impact if a risk materializes	**Slight**
	Number of affected users: The number of users affected by over-blocking would be limited to the content creators that have uploaded the material. Visitors are unlikely to experience any issues if content they viewed previously is now blocked – Slight
	Irreversibility of the damage: Putting back content that has been over-blocked would remedy the issue. – Slight
Probability The likelihood of the risk materializing	**Improbable**
	The risk is improbable due to mitigating factors.
Overall assessment	**Low**

Mitigating measures in place

Identity and consent

There are two types of uploaders on Pornhub: individual content creators, often referred to as "Models", and content partners, or third-party professional content studios.

As part of their registration, content partners are required to provide a company name, company/studio content website, and physical address or URL indicating the coordinates of their custodian of 2257 records (pursuant to record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content).

Every new uploader is required to undergo identity verification with a third-party identity verification provider, which requires them to:

- Submit a government-issued ID, which is authenticated by the provider.
- Conduct a liveness test to ensure the users likeness matches the government-issued ID and they are one and the same person.
- The liveness test also ensures that the person is alive and real, not AI, not pre-recorded, not a still image.

At time of signup, and again at the time of each upload, all uploaders are required to attest that they have obtained and retained ID and consent to record and distribute content from all other performers appearing in their content.

As part of Pornhub's more extensive verification processes, for individual content creators, these requirements are validated at least once per additional performer:

- Uploaders may meet the ID and consent verification requirement for their Co-performer in one of the following ways:
    - ID and liveness (biometric) test per above, plus signed consent form upload. Our internal moderators review the result of the ID and liveness, and the terms of the consent form.
    - Upload a photo and ID plus signed consent form. ID is validated by a third party ID validation service, with our internal moderators verifying the result of the ID validation, that the face of the co-performer matches the ID, and the terms of the consent form.
    - ID and Release form package. Upload copies of photo, ID, and signed consent form which is then reviewed by internal moderators, verifying the face of the co-performer matches the ID and the terms of the consent form.
    - eSign (provided by Yoti). Co-performer undergoes ID, liveness (biometric) and performs e-signature of consent form. If co-performer ID has been uploaded separately previously, this option also supports reduced steps, with just the liveness and e-signature.
    - Existing content creator. Where two or more registered and verified content creators feature in the same content, they are able to tag each other, requiring affirmative consent.
- All co-performers must be approved by a member of the moderation team. All performers appearing in uploaded content are checked by moderators against approved co-performers, to ensure everyone appearing in content uploaded by content creators can be matched to an ID-verified and approved co-performer. If there is any doubt then further documentation will be requested from the uploader before the content is published. For example, if the content does not feature a face that can be compared to the identity documents, then further images may be required to ascertain that they are the same person. Ensuring identity and age of performers are verified and validated before publication severely limits the risk of potentially illegal material from upload.
- Note, some older content on the platform fell under an older policy where the content creator was required to attest to having ID and consent records for co-performers but before the company began validating either one or both requirements for all content prior to publication. However, per the timeline near the beginning of this document, we have announced a 30 June 2025 deadline for individual verified uploaders to submit ID and consent paperwork for co-performers in previously uploaded content. Older videos that do not meet our current verification requirements will be removed from the platform by that date. For details, see our blog post.
- Content partners must first go through an on-boarding process (see **Annex 1 – CPP Onboarding Process v1.2**).
- As it relates to content partners, Studio produced content follows record-keeping requirements for age and identity verification under 18 U.S. Code § 2257, which requires creating and maintaining individually identifiable records pertaining to every performer portrayed in a visual depiction that comprises adult content.. While their website(s) and sample ID and consent paperwork are audited at onboarding and annually they are not required to provide us with IDs for

all performers prior to content publication. This part of the verification process is managed by the studios, and they are required to provide all documentation on demand:

  - Content partners are required to go through a KYC process to validate their identity and business. (see **Annex 2 - KYC Process V1.1**)
  - All content partners go through an annual audit where they are required to provide documentation for a random selection of their content.

- Further information on the verification process can be found in the following documentation:
  - How to Sign Up and Join the Model Program – Pornhub Help , including the video tutorial on this page
  - Yoti Tech documentation: Overview - Yoti developer documentation
  - Yoti Demo: Yoti Identity verification
- We have also now added INCODE as an additional identity verification provider.
- This robust process deters and helps to mitigate the risk relating to the upload of illegal material, or committing any illegal acts on the platform.
  -

Human checks of all removed content

- Any content which is reported or flagged for removal is investigated by a human support team. The support team will contact the content creator if there is any doubt that the content is illegal or does not have the consent of performers. This helps prevent over-blocking as a dialogue is created with the uploader, giving them the chance to discuss the removal and provide anything required by our support team in order to allow the content to be re-published.
- Content creators may also use this dialogue to appeal any decision if they are able to provide new information that was not already considered when removing their content.

Gender-based violence, public health, minors, physical and mental well-being

Negative effects in relation to minors

The effect of pornography on minors is subject to an ongoing comprehensive discussion in psychology and sociology. The same goes for the implications, including their advantages and disadvantages, of some mitigating factors and in particular for the various forms of age verification. The essence of these discussions is important to assess the risks as well as any mitigating factors appropriately. In the following, we will address the most recent findings regarding the severity of impact of pornography on minors and also deal with the repercussions and risks related to different forms of age verification. Both topics – severity of impact as well as certain adverse consequences of age verification – are closely related as care must be applied to not increase the overall risk exposure of minors by applying inappropriate forms of age verification.

1. Effect of Pornography on Minors according to latest Studies

Whilst there is wide agreement that pornography is not suitable for minors in general, the specific impact on different groups of minors (adolescents and pre-adolescents in particular) as well as their different level of exposure is relevant for a subsequent risk evaluation as well as the appropriate mitigating factors.

- In her book of 2023 *Porno – an Analysis without Shame,* Madita Oeming addresses the effects of pornography on society and individuals in a very comprehensive manner. Chapter IV (page 82 onwards) deals with the effects on minors and is summarized as follows (page 91):

  > *"The findings show that young people are aware of pornography and specifically seek it out. Porn is not a niche phenomenon, but a widespread form of adolescent media use. Pre-pubertal children, however, rarely actively search for pornographic content and contact, if at all, tends to be unintentional. Their own interest usually awakens with the onset of puberty, increases continuously and then often levels off again in adulthood. Just like the age of onset, the extent of adolescent porn use is often overdramatized in the media. Although porn is part of the realities of young people's lives, it is not a primary topic of conversation for them and plays a rather subordinate role compared to other media offerings such as Instagram, TikTok and YouTube formats or computer games such as FIFA or Fortnite."*

- In a similar vein, the British Board of Film Classification (BBFC) determines it in its 2020 study Young People, Pornography & Age Verification (British Board of Film Classification (BBFC), January 2020, Young people, pornography & age-verification page 30):

  > *"Many young people in the qualitative research turned to pornography to understand sex and what it might entail"* (p. 30).

- A similar observation follows from Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo, p. 93, concluding:

  > *"As the results showed, a substantial number of children were positive about their experience. This is also in line with the presumption that children use the internet to fill their developmental needs."*

Whilst this does not suggest that pornographic content is suitable for minors, it does indeed suggest that any potentially negative implications do not seem to be perceived as such.

- In addition, in times of a generally heteronormative society, queer teenagers are often neglected, thus one of the only support in ascertaining and confirming their identity and place in society is pornographic content. The BBFC study confirms this by stating "*almost half of all LGB respondents felt that pornography had helped them to understand their sexuality*" (p. 34).

2. Repercussions and Implications of different Forms of Age Verification

There are different methods of verifying the age of a website user. Those methods currently available on the market that provide a high degree of certainty that a given user is indeed of age, will either need to verify the user's identity (either directly or by means of a third party verifying agent) or apply AI based, real time biometric screening. Applying either of these methods will typically have the following implications:

- According to all available evidence and as for example shown by the UK survey of the YouGov institute, the great majority of all users (78 % in the case of the UK survey) are unwilling to undergo any such form of age verification on adult platforms, see Aloha press release. Our own experience proves the same point: The implementation of strict age verification through ID checks on Pornhub for users residing in Louisiana on 1 January 2023 lead to an immediate loss of over 80% of our traffic.

- The users leaving Pornhub when required to do age verification do not simply stop watching pornography. They instead go to any one of a thousand other available online offerings without any protection of minors, and typically also without any other protections against other forms of risks. This migration of user traffic to other adult sites – caused by such a strict age verification process of the most protective site, such as Pornhub – is much more harmful for affected minors, as to the best of our industry knowledge, almost every single one of the thousands of alternative available sites offering pornographic content is less regulated, as well as less compliant, than Pornhub. Most of these providers of adult content have no measures in place at all to protect minors and ensure a safe and legal environment for their users. That is in clear contrast to Pornhub's own compliance, shown by our range of robust trust & safety measures. The Canadian Centre for Child Protection also noted that our reporting options, which have since improved further, were better than many mainstream platforms, set out in Canadian Centre for Child Protection, 2020, Reviewing child sexual abuse material reporting functions on popular platforms, p. 10.

- In addition to such mass migration to significantly less compliant and outright non-compliant sites, strict age verifications implemented in certain jurisdictions could be circumvented by using VPN-clients, which studies have proven to be known by minors nowadays (see Newswire Article, quoted above and British Board of Film Classification (BBFC), January 2020, Young people, pornography & age-verification, p. 56).

- Independent from the points just raised above, strict age verification systems are also in conflict with existing data protection laws in the EU and in particular the GDPR. Collecting detailed personal user information at site level undermines the principles of data minimization, Art. 5 and 25 GDPR. Several data protection authorities in the EU have made this point already:

    - For example, the French data protection authority *Commission Nationale de l'Informatique et des Libertés* (CNIL) states in its publication of 22 September 2022

regarding Online age verification: balancing privacy and the protection of minors: "*The CNIL has analysed the main types of age verification systems in order to clarify its position on age verification on the Internet, particularly on pornographic sites for which such verification is mandatory. It specifies how such publishers could fulfil their legal obligations. However, CNIL finds that such current systems are circumventable and intrusive, and calls for the implementation of more privacy-friendly models*."

- A similar conclusion was drawn from the English data protection authority back in 2017 regarding the Digital Economy Act and the implementation of strict age verification systems, as this article shows: "*With the passing of the Digital Economy Act 2017, the United Kingdom became the first country to pass a law containing a legal mandate on the provision of an Internet age verification system. Under the act, websites that published pornography on a commercial basis would have been required to implement a "robust" age verification system to prevent minors from accessing their sites. […]. Key issues with the implementation included what constituted an effective means of age verification, as well as concerns over the possibility that online age verification providers could collect excessive personally identifiable information and process it for other purposes—potentially in violation of the General Data Protection Regulation (GDPR).*"

- The privacy risks of age verification were highlighted recently by the Australian government who decided not to proceed with mandatory platform-level age verification. As well, in 2023 Texas introduced a law whose stated goal was to prevent the publication or distribution of sexual material to minors on the internet to prevent minors from accessing age-restricted content on the internet. A US Federal Judge in Texas rightly found that the bill's age verification process, other restrictions and information requirements violated Texans' freedom of speech, raised privacy concerns, and was overly broad and vague. A similar law targeting social media platforms in Arkansas was also judged unconstitutional around the same time.

- In Spain, the national Data Protection Authority published in its Decalogue an endorsement of device level age verification methods – specifically with a view to the privacy concerns of platform based strict age verification methods: "*It is also necessary to remove, from the design, the impact that personal data breaches of third-party verification services or Internet services could have on minors. A possible* solution *is to* ***process the identity information, the "authorized to access" condition and the execution of access limitation policies on the devices held*** *by users without relying on the servers of the service providers or third parties. In this sense, the requirements of* ***Article 25.2 of the GDPR regarding the minimization of personal data must be considered***."); "*The system for protecting minors from inappropriate content must prevent third entities from acting as intermediaries between the user and the Internet service provider using strategies that allow identification, browsing monitoring and/or profiling of the person.* ***This could be achieved, for example, by providing tools so that the personal device is the one that executes all the verification mechanisms without using external resources, including the execution of content access limitation policies on the same device****. Another strategy could be that the identity providers provide accreditation of the "authorized to access" condition unlinked with the user identity, that the aim to access adult content is not linked to the user, and that the process to get the accreditation does not generate meta-information linked to the person.*"; and "***Executing access restrictions locally on Internet users' devices would eliminate the risks of profiling or monitoring***" (page 8; in bold by us).

Severity The amount and extent of negative impact if a risk materializes	**Slight - Marginal**

Affected users: Access to Pornhub is not allowed for any users below at least 18 years of age, or the age of majority in their respective jurisdiction, as is stated at the outset of our Terms of Service at https://www.pornhub.com/information/terms. Before accessing Pornhub, users must confirm that they have reached the required age. For further details, see below on mitigation measures in place on Pornhub.

Further, Aylo does not collect any mandatory age data on its users for Pornhub (or for its other cost free video sharing sites), nor does the DSA (or any other regulation) require it to do so, see Art 28 (3) DSA. This is reconfirmed in Recital 10, which clarifies that:

"The protection of individuals with regard to the processing of personal data is governed solely by the rules of Union law on that subject, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC."

With regard to the potential presence of minors on its platform, and their proportion in relation to adult users, Aylo must therefore resort to general statistics on access of adult content sites by minors. Since these statistics are overwhelmingly informed by the prevalent number of sites without any age assurances in place, they are by necessity highly imprecise and do no not reflect the realities on Pornhub. That said, the following general trends can be observed:

- Children before the age of adolescence: according to the general findings with regard to all adult websites (not specific to Pornhub), the number of pre-adolescent children visiting pornographic websites is very low. In addition and most importantly any such visit would not be Pornhub specific meaning that the overall amount of visits to just any site with pornographic content would not change or alter – irrespective of the availability of Pornhub.
- Adolescents: in the absence of specific numbers for Pornhub, it can be derived from the general surveys as referenced in the background text that with increasing age of adolescence, the visit of pornographic sites will rise as a considerable part of older adolescents will proactively seek out pornographic content on the internet. Any such visit would, however, not be Pornhub specific meaning that the overall amount of visits to just any site with pornographic content would not change or alter – irrespective of the availability of Pornhub.

	Irreversibility of the damage: • Minors only accessing the platform accidentally: no damage, the situation can be reversed completely as soon as the minor leaves the platform – also due to existing risk mitigation methods (see below) – Slight • Minors consuming pornographic content: the (possible) damage and situation can be remedied by subsequent sexual education and open communication – Marginal
Probability The likelihood of the risk materializing	**Improbable – Remote**
	In line with the points set out above, there is a certain probability that adolescents will end up – in line with their intent – on Pornhub. However, any such visit would not be specific to Pornhub given the omnipresence of sites with comparable content (albeit less compliant content and with insufficient content moderation procedures in place). Accordingly, there is a certain probability for this risk to materialize – but this materialization is independent from Pornhub. In summary: • minors only accessing the platform accidentally: remote • minors consuming pornographic content: improbable (that a minor access PH **and** because of that suffers a damage).
Overall assessment	**Low to medium**

Mitigating measures in place

Implementation of RTA-Label

- Aylo has voluntarily implemented the "Restricted to Adults Label" on Pornhub (and across our other adult content sites), which is a self-labeling initiative for adult content websites. Developed by the Association of Sites Advocating Child Protection (ASACP), the RTA label is designed to enable parental filtering:
    - Websites that carry the RTA label display an RTA tag in their HTML code. Operating systems, browsers, and parental filtering software can recognize this tag and block access to the website for users under the specified age limit.
    - Thus, parents can easily make use of parental control systems by using one of the many available options given by operating systems or filtering software and manage them individually on their children's phone, laptop, tablet or other device. The system also adheres to the GDPR principle of data minimization as it does not require any user data to be shared with anybody else, including Pornhub or any third party (age verification) agent.

- The RTA-Label is therefore enormously better suited for the protection of minors than strict age verification systems (i.e. identity verifying systems). Strict age verification systems can be circumvented by using VPN-clients. In contrast, RTA-Labels work independently of the user's IP address or location, as they filter content based on categorization.

Age verification by self-declaration

- As mentioned above, we furthermore apply a self-declaration method to verify a user's age before a user can access the content on our site:
- The required statement confirms our users' adherence with the requirements of our Terms of Service, which require all users to be at least 18 years old, or the age of majority in their respective jurisdiction (where that should be higher), see https://www.pornhub.com/information/terms. In addition, the age confirmation requirement also serves as a psychological deterrent, cautioning minors to act in a compliant manner and refrain from accessing Pornhub.

Sexual Wellness Center

- Our Sexual Wellness Center deals with many sexual health topics in an open, honest, and educational manner. It contains hundreds of articles from leading experts, written specifically for the Center. The Center's main contributor, Dr Laurie Betito, conducts multiple Q&As and hosts a podcast on a variety of sexual health subjects using questions posed by visitors to the site. Regarding protection of minors: the Sexual Wellness Center on the platform is thus a great possibility for minors interested in sexual education to inform and educate themselves without the necessity to consume pornographic content.

Future mitigation measures

We believe that the real solution for protecting minors and adults alike is to verify users' ages at the point of access – the users' devices – and to deny or permit access to age-restricted materials and websites based on that verification*.

This approach requires working with operating system companies and, with their buy-in, stands to minimize the transmission of personal data while protecting minors from age-restricted content across the entire internet.

We support device-level age verification because it would control the severe risks inherent with potentially having hundreds of thousands of sites introducing and holding their own age verification systems and require consumers to repeatedly present their ID or undergo biometric processing.

The technology to accomplish this exists today. Many devices already offer free and easy-to-use parental control features that can prevent minors' accounts from accessing adult content without risking the disclosure of sensitive user data. These features simply need to be mandated to block devices by default, unlocked only by age verification by an adult on the device.

Apple introduced age verification into their services. According to Apple's announcement, as of fall 2023, "businesses will be able to accept IDs in Apple Wallet — no additional hardware needed. This will streamline their ability to securely check a customer's age in person for things like alcohol purchases or to verify a customer's identity at checkout for car rentals, and more."

We support the “opt-out” approach wherein age-based blocks on inappropriate content would be default-on and would require a verified adult to turn the filter off. This far exceeds the current “opt-in” patchwork approach in which only a fraction of sites hosting age-restricted content have any kind of age-gating or content-blocking options available to help parents effectively block their children from accessing.

The device level solution is 360-degree solution that stops age-restricted content at the source and protects a user’s privacy by not requiring users to provide their PII on multiple-sites across the internet.

Age verification at the device level provides the strongest protection possible to block minors from accessing inappropriate sites, protects adult user privacy, and is enforced equitably across all platforms.

**Device-Based Age Verification refers to any approach to age verification where the personal information that is used to verify the user’s age is either shared in-person at an authorized retailer, inputted locally into the user’s device, or stored on a network controlled by the device manufacturer or the supplier of the device’s operating system. Whether through pre-installed content blocking and filtering software, the disabling of web-browsing permissions, or other means, the user will then be prevented from accessing age-restricted content over the internet unless they are age-verified. To come to fruition, such an approach requires the cooperation of manufacturers and operating-system providers.“*

Porn addiction

There is little agreement by those in the psychology field, that porn addiction is a treatable problem. In fact, many studies suggest that porn addiction is a symptom of a deeper problem.

- Is Porn Addiction Really a Disorder? | Psychology Today

  "The problematic porn or self-described "porn addiction" use can be viewed more as a symptom of deeper psychiatric issues and/or relational conflicts the person has with others."

- Science Stopped Believing in Porn Addiction. You Should, Too | Psychology Today

  "Having moral conflict over your porn use (PPMI) does turn out to be bad for you. But that's not because of the porn. Instead, higher levels of moral conflict over porn use predict higher levels of stress, anxiety, depression, and diminished sexual well-being, as well as religious and spiritual struggles"

Severity The amount and extent of negative impact if a risk materializes	**Slight – Marginal**
	The effects and intensity of a possible porn addition vary. This and the conflicting opinions of experts aggravate measurement. – Slight – Marginal
	Irreversibility of the damage: Cessation of porn use can help remedy and restore the prior situation – Marginal
Probability The likelihood of the risk materializing	**Remote**
	The risk of a person becoming addicted to pornography appears to be based upon multiple external factors, not least their moral objection to pornography – Remote
Overall assessment	**Low – Medium**

Mitigating measures in place

Sexual Wellness Center

- Our Sexual Wellness Center deals with many sexual health topics in an open, honest, and educational manner. It contains hundreds of articles from leading experts, written specifically for the Center. The Center's main contributor, Dr Laurie Betito, conducts multiple Q&As and hosts a podcast on a variety of sexual health subjects using questions posed by visitors to the site.
- Regarding addiction the center contains:

- Podcast: Is Porn Addiction Real? In this episode of the podcast, Dr. Laurie discusses the question, “Is Porn Addiction Real?
- Podcast: Sex Addiction Is On The Rise In this podcast episode, Dr. Laurie discusses how sex addiction is on the rise with guest David Essel.
- Understanding Sex Addiction This video challenges the use of the words “sex addict” and explains why sex addiction, at least as a mental health definition, does not exist as well as how it stigmatizes any sex that is deemed “wrong” by our culture. Instead, I talk about sexual behavior that feels out of control, what to do about it, and how to get support from a professional who will not shame diverse sexual practices.
- Q&A With Dr. Laurie: When Does It Go Too Far?

Negative effects on relationships

Pornography usage in relationships can present positive and negative effects and a key factor appears to be an individuals moral opinions on pornography.

How Porn Affects Relationships | Psychology Today – *"In the end, it appears that whether porn viewing helps or hurts intimate relationships depends instead on the attitudes the partners have about it. If you already believe porn to be evil, you'll likely suffer guilt and remorse over your own use, as well as feelings of anger and betrayal over finding your partner using it. But if you have open and healthy attitudes about your own and your partner's sexuality, then you're likely to use porn in ways that enhance your relationship with your significant other.*

How Porn Affects Relationships | Psychology Today – *"The most important finding to come out of the data analysis was the fact that porn use was completely unrelated to relationship satisfaction. In other words, there was no evidence that porn viewing led to decreases in how happy people are with their partners, nor did they seem to be using porn as a way of making up for deficiencies in their relationships".*

Severity The amount and extent of negative impact if a risk materializes	**Slight - Marginal**
	Affected viewers: The number of factors influencing relationships are manyfold. We are not aware that the use of Pornhub has a notable impact on relationships – Slight – Marginal
	Irreversibility of the damage: Cessation of porn use can help remedy and restore the prior situation – Marginal
Probability The likelihood of the risk materializing	**Remote**
	The risk of a person's relationships being affected by their pornography usage appears to be based upon multiple external factors, not least their moral objection to pornography – Remote
Overall assessment	**Low – Medium** The risk of pornography use affecting relationships is not something which can be fully mitigated as it stems from other problems in a person's life.

Mitigating measures in place

Sexual Wellness Center

- Our Sexual Wellness Center deals with many sexual health topics in an open, honest, and educational manner. It contains hundreds of articles from leading experts, written specifically for the Center. The Center's main contributor, Dr Laurie Betito, conducts multiple Q&As and hosts a podcast on a variety of sexual health subjects using questions posed by visitors to the site.

- Regarding relationships the center contains:
    - Is Porn Cheating? Watching porn can be great and even fun if you view it as a movie, and if everyone in the relationship is okay with it. However, if you notice your partner sneaking around to view porn, it would be good to discuss “is porn cheating?” instead of accusing him/her of cheating. Remember that communication in the relationship is the most important thing, and don’t be afraid to ask for professional help if you think it is necessary.

Pornography fostering abuse and violence

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected viewers: Anyone who sees it. The reach depends upon how long the material remains on the site and the number of views – Critical
	Number of affected victims: The number of victims is limited – Low
	Irreversibility of the damage: Removal can remedy, but will not remove the negative impact on those who saw it or those within it – Critical
Probability The likelihood of the risk materializing	**Improbable**
	The risk is improbable due to mitigating factors. Our latest voluntary transparency report – 1 July 2024 – 31 December 2024 shows that the content removed for violence is low, therefore showing the lack of prevalence of such material on the platform: In the last six months of 2024, we removed 451 pieces of content (411 videos and 40 photos) for violating our bodily harm and violent content policy.
Overall assessment	**Medium**

Mitigating measures in place

Policies

- We do not permit violent or abuse content on our platforms, as detailed in our Violent Content Policy.

Banned Words List

- The platform utilises a database of banned words and phrases, which are prevented from being entered into any user-input fields, including titles, descriptions, tags, playlists, and searches. The database contains words and terms from multiple sources, including NGOs, Law Enforcement, and the platforms own.

Contextual Text Moderation

- Users can comment underneath videos presented on the platform. These comments are moderated using third-party software from Spectrum Labs AI. The software scans comments in a contextual manner, for multiple bad behaviours including violence. Any volitive comments are

automatically removed from the platform. This further reduces the likelihood of violent material, even in written form, from appearing on the platform.

Human moderation

- All uploaded images and videos are reviewed by at least one human moderator before being published on the platform. Human moderators check that the IDs provided by uploaders and performers match those within the material. If there are any concerns, then the moderator will reach out to the uploader to supply more information and documentation. Human moderators use the results from all tools to assist them in assessing the content and only publish material once they are confident that the material does not violate our policies and guidelines. Requiring moderation of all images and videos before publication, severely limits the likelihood of any foreign interference.

Content Removal Request

- A content removal request form (**CRR**) is linked at the bottom of every page on the platform. All visitors to the platform can use the CRR to report material by providing the URL of the content, the reason why it should be removed, and an email address so that the platform can communicate with the reporter, ask for more detail if required, and confirm our decision. Content reported in this manner is immediately and automatically removed, once the reporter has confirmed their email address. This reduces the risk of viewing material and limits harm to victims.

Content Flagging

- The platform offers another way for logged-in users to flag all images, videos, comments, and users. Content flagged in this manner will be reviewed by a moderator within just a few hours and de-published if it is found to violate our Terms of Service. This reduces the risk of viewing material and limits harm to victims.

Law enforcement portal

- We host a law enforcement portal so that law enforcement is able to quickly request information from the platform to assist with legal cases.

Freedom of Sexual Expression

- When acted out by consenting adults in safe environments and adhering to our Terms of Service, desires, fetishes and fantasies are welcomed and supported on our platform. Pornography does not always represent sexual interactions and behaviours typical of everyday life, and can depict diverse fantasies and role-play by consenting amateurs and professionals.

Sexual Wellness Center

- Our Sexual Wellness Center deals with many sexual health topics in an open, honest, and educational manner. It contains hundreds of articles from leading experts, written specifically for the Center. The Center's main contributor, Dr Laurie Betito, conducts multiple Q&As and hosts a podcast on a variety of sexual health subjects using questions posed by visitors to the site.
- Regarding abuse the Center contains: How To Date After An Abusive Relationship.

Other resources

- As violent and abuse content is also likely to be non-consensual, please also see our risk assessment on non-consensual content (**NCC**).

Frustration due to unrealistic expectations

When acted out by consenting adults in safe environments and adhering to our Terms of Service, desires, fetishes and fantasies are welcomed and supported on our platform. Pornography does not always represent sexual interactions and behaviours typical of everyday life, and can depict diverse fantasies and role-play by consenting amateurs and professionals.

Learn more about our Core Values.

Severity The amount and extent of negative impact if a risk materializes	**Slight – Marginal**
	Affected viewers: The impact on users that may left frustrated due to their unrealistic expectations of sex based upon pornography usage is unclear – Slight – Marginal
	Irreversibility of the damage: There will be some remedying of potential damage if a user ceases to watch the pornography that they believe is frustrating them – Marginal
Probability The likelihood of the risk materializing	**Remote**
	The risk of a person gaining unrealistic expectations based upon pornography viewing is unknown and differ individually – Remote
Overall assessment	**Low – Medium** The risk of pornography use leading to unrealistic expectations cannot be fully mitigated. Pornography is legal and should allow freedom of sexual expression.

Mitigating measures in place

Freedom of Sexual Expression

- Freedom of sexual expression is one of our core values, and we make clear that pornography does not always represent sexual interactions and behaviours typical of everyday life.
- It is important for content creators to be permitted to post content within the bounds of our terms of service in order to allow freedom of sexual expression.
- In mainstream media, depictions of realistic illegal acts are permitted under the form of entertainment, e.g. violent murders within multiple Hollywood movies and TV shows. Our platform does not feature any illegal acts but are presented with the understanding that a viewer should treat the content as a fantasy, not reality.

Sexual Wellness Center

- Our Sexual Wellness Center deals with many sexual health topics in an open, honest, and educational manner. It contains hundreds of articles from leading experts, written specifically for the Center. The Center's main contributor, Dr Laurie Betito, conducts multiple Q&As and hosts a podcast on a variety of sexual health subjects using questions posed by visitors to the site.
- Regarding unrealistic expectations the Center contains:
    - Q&A With Dr. Laurie: Expectation Vs Reality (pornhub.com)
    - Q&A With Dr. Laurie: Fantasy Vs. Reality (pornhub.com)

Overarching factors

Ad delivery

Our advertising is subject to the same controls as our content, i.e. a plethora of moderation tools and human moderation before adverts can be offered on the platform.

We permit advertising from NGOs who provide services to help change problematic user behaviour (e.g. those looking for CSAM or NCC), which is displayed across our platforms in multiple geos.

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected viewers: If our ad delivery system were to promote illegal, harmful material then the risk would be critical.
	Irreversibility of the damage: The situation can be largely reversed if the adverts are removed from the platform in time.
Probability The likelihood of the risk materializing	**Improbable**
	Due to the mitigation measures we have in place, the risk is improbable.
Overall assessment	**Medium**

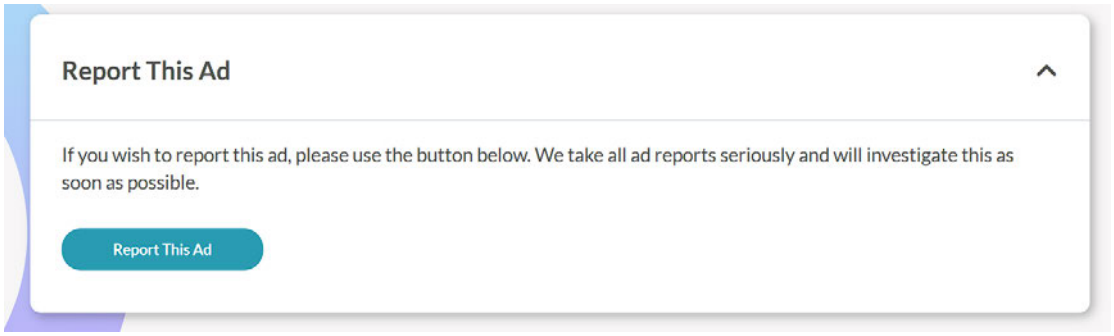
Mitigating measures in place

Preventing harmful material

- All our advertising is subject to moderation prior to being published on the platform.
- Please see our robust mitigation measures already in place per our risk assessments on dissemination of illegal harms.

Reporting

- All users (logged in or not) can report adverts that they believe contain illegal, inappropriate or copyright material. This is achieved by clicking on the "Ads" portion of the advert in the top right corner and then choosing Report this Ad.


Report This Ad
If you wish to report this ad, please use the button below. We take all ad reports seriously and will investigate this as soon as possible.
Report This Ad

Recommender systems

Theoretically, a risk regarding recommender systems can be to amplify the visibility of illegal and/or harmful material.

The content on our platform is carefully moderated using a plethora of tools and human moderation.

Our recommender systems cannot push people towards illegal, harmful material due to the robust moderation tools we have in place. The likelihood of such content existing on our platforms is very low, contrary to what may occur on social media platforms.

Severity The amount and extent of negative impact if a risk materializes	**Critical**
	Number of affected users: If our recommender system were to recommend illegal, harmful material then the risk would be critical.
	Irreversibility of the damage: The situation can be largely reversed if the content is removed from the platform in time or by an affected user turning off the recommender system.
Probability The likelihood of the risk materializing	**Improbable**
	Due to the mitigation measures we have in place and the inherent nature of our platform (not a social media platform), the probability of risks associated with our recommender system is improbable.
Overall assessment	**Medium**

Mitigating measures in place

Preventing harmful material

- Please see our robust mitigation measures already in place per our risk assessments on dissemination of illegal harms, many of which far exceed those used on social media platforms. Two important aspects to note are:
    - Our banned words service which proactively blocks searches for illegal material, despite our platform having a very low change of offering such content in the first place.
    - Deterrence messaging, which is returned against a large list of banned words associated with certain types of illegal material, so that users are educated on the illegality and can seek help from one of our NGO partners to change their behaviour.

Ability to turn off recommender systems

- As detailed in our guidelines, a user can turn off personal recommendations by selecting the option in the hamburger menu on the platform. (See Recommender System Guidelines (pornhub.com))