Protecting people from illegal harms online

Draft Updated Illegal Content Judgements Guidance (ICJG) (relevant extracts)

Consultation

Published 25 November 2026

1. Image-based adult sexual offences

Warning: this chapter contains content that may be upsetting or distressing

Priority image-based adult sexual offences

1.1 This chapter considers image-based sexual offences which involve adults, that is persons aged 18 and over. The priority image-based adult sexual offences comprise:

a) Possession of extreme pornographic images

b) Offences related to non-consensual disclosure of intimate images (intimate image abuse)

c) Sending or giving a photograph or film of the genitals with the intention of causing alarm, distress or humiliation, or for the purpose of sexual gratification on the behalf of the sender ('cyberflashing').

1.2 The Act also covers offences of encouraging and assisting the commission of image based adult sexual offences and conspiracy to carry out possession of extreme pornographic images and intimate image abuse.

1.3 For more information on harms relating to image-based adult sexual offences see the following chapters of the Register of Risks: the chapter titled 'Extreme pornography,' the chapter titled 'Intimate image abuse' and the chapter titled 'Cyberflashing'.

Age and the image-based sexual offences in this chapter

1.4 While children can be victims or survivors of both the intimate image abuse offence and the cyberflashing offence, the typically sexual nature of the offences in question mean that any content which involves a child and meets the threshold for an offence mentioned above will usually automatically amount to a child sexual exploitation and abuse (CSEA) offence.[1] A piece of extreme pornography involving a child would automatically be classed as child sexual abuse material (CSAM).

1.5 A CSAM offence is committed when an indecent image of a child is created. See Chapter 4 of this document, 'Child sexual abuse and exploitation (CSEA): offences relating to child sexual abuse material (CSAM), for more information.

Extreme pornography

1.6 If the content in question involves adult nudity or image-based sexual content, service providers should first ask whether it amounts to an extreme pornographic image.[2]

[1] In the case of intimate image abuse, the offence in question would be the sharing of indecent images of a child. In the case of cyberflashing, the content in question would likely amount to sexual communication with a child if sent by an adult. If the cyberflashing image was of a child, it would be classified as an indecent image of a child.

[2] Under section 59(3)(b) of the Act, content is illegal content if its possession amounts to an offence.

What is an 'image'?

1.7 Both still images and moving images such as videos are encompassed within the definition of an 'image'. Data which is capable of being converted into an image or video, such as compressed image files, should be treated as equivalent to the image itself. Content which itself does not consist of an image but which consist of a URL linking to such an image should also be treated as equivalent to the image itself.

What is extreme pornography?

1.8 For content to be 'extreme pornography' it must:

a) be pornographic, that is of such a nature that it must reasonably be assumed to have been produced either solely or principally for the purpose of sexual arousal;
b) be grossly offensive, disgusting or otherwise of an obscene character;
c) involve persons or animals that a reasonable person would think were real upon inspection of the image; and
d) portray one or more of the following acts in an explicit and realistic way:

i) an act which threatens a person's life (see below);
ii) an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals;
iii) an act which involves sexual interference with a human corpse (necrophilia);
iv) a person performing an act of intercourse or oral sex with an animal, whether dead or alive (bestiality);
v) an act which involves the non-consensual penetration of a person's vagina, anus, or mouth by another person's penis; or
vi) an act which involves the non-consensual sexual penetration of a person's vagina or anus by a part of another person's body or anything else.

1.9 All four of the above criteria (a) to (d) must be met in order for the image in question to be an extreme pornographic image.

1.10 Service providers should note that simulated acts, including acts depicted in synthetic images such as 'deepfakes', fall within the above definition, provided they are depicted in an explicit and realistic way.

'Pornographic'

1.11 Whether content can be assumed to have been produced either solely or principally for the purpose of sexual arousal is dependent on the nature of the image itself, not the intent of the person posting the content or any viewer of it.

'Grossly offensive, disgusting or otherwise obscene'

1.12 'Grossly offensive' should be given its ordinary meaning. 'Obscene' should also be given its ordinary meaning.

'Explicit and realistic' portrayal

1.13 The requirement that the acts in question should be portrayed in an 'explicit and realistic way' means that artistic depictions which are not lifelike in character are unlikely to meet this criterion. For example, a manga drawing would not be realistic enough. However, synthetic, simulated, edited or manipulated images or videos such as 'deepfakes' which retain a realistic character are likely to satisfy this criterion where they depict the acts mentioned above.

Acts which threaten a person's life

1.14 'Acts which threaten a person's life' mean acts which depict physical endangerment with a material risk of death. Non exhaustive examples include explicit and realistic hanging, strangulation, suffocation and causing life threatening injury.

Non-consensual sexual penetration

1.15 'Non-consensual penetration' means that the person being penetrated did not or could not consent to the act in question. Examples where consent to penetration cannot not be given include when a person is asleep or otherwise unconscious, or where the penetration results in serious harm.

1.16 We recognise that inferring consent in these cases is very complex. Where appropriate, service providers should take into account contextual information such as content titles or descriptions, or statements from those depicted in the content, when making a judgement as to whether the acts depicted are non-consensual. A user report which suggests that the content depicts non-consensual acts should be taken as reasonable grounds to believe that there was no consent, unless there is evidence to the contrary.

State of mind

1.17 The state of mind requirement for this offence can be assumed to be met by virtue of the image, or a URL linking to the image, being posted.

Relevant defences

1.18 Content which meets the criteria set out above should not be considered illegal where there are reasonable grounds to infer that either of the following is true:

a) the user in question (that is, the user uploading the image or otherwise making it available on a user-to-user service or website) has a legitimate reason for being in possession of the image concerned; or
b) the image is an 'excluded image'.

1.19 Legitimate reasons are not set out in statute and providers should use their discretion when considering reasons given on a case-by-case basis. However, it should be noted that legitimate reasons given for possessing the content personally or where it can be accessed only by users with the same reasonable excuse may not extend to or justify the hosting of such an image on a public platform. The service provider would need reasonable grounds to infer that each viewer of the content has a legitimate reason in order for the content not to be illegal content.

1.20 It should be noted that malicious intent is not needed for content to amount to an offence. Jokes in poor taste should still be considered as illegal content, as should content posted for the purpose of exposing an offender or offenders.

1.21 An 'excluded image' is an image or video taken from a work classified by the British Board of Film Classification (BBFC). If the content being considered is taken from a classified work, the content may not be illegal, except in cases where the content could reasonably be assumed to have been 'extracted' in such a way that it may be reasonably assumed to be solely or principally for the purposes of sexual arousal.

Encouraging, assisting and conspiracy to possession of extreme pornography

1.22 As set out above, encouraging and assisting the possession of, and conspiracy to possess, extreme pornographic images are also priority offences. In all these cases, content which amounts to the encouragement assistance, or conspiracy will only be illegal content to the extent that the possession of extreme pornography which is being encouraged, assisted or conspired to is sufficiently linked to the UK – the question is whether the UK would prosecute the people involved. The rules which decide whether or not there is a sufficient link are very complicated and content moderators cannot be expected to understand them in detail. However, for the purposes of this guidance, content should be considered illegal if the person being encouraged or assisted, or with whom there is a conspiracy, is either British or located in the UK.

1.23 Encouraging could include words urging another person to carry out the offence. Assisting could include providing substantive help in carrying out the offence. There must either be intent to encourage/assist the offence, or belief that the offence will be committed. For conspiracy, there must be an agreement between two people and intent to carry out the offence.

Risk assessment and extreme pornography content

1.24 For the purposes of carrying out a risk assessment, providers should be aware that (priority) illegal content which amounts to the offence of publishing extreme pornography may take the form of a videos or images (including those which have been digitally manipulated i.e. deepfakes), or links to these same videos or images.

1.25 Content amounting to these offences may be found on user-to-user services (including user-to-user pornography services and messaging services). Search services may also be used to search for and access such content, for example via video or image viewing facilities.

1.26 See the Register of Risks chapter titled ‘Extreme pornography’.

Usage examples

A video posted to a social media platform depicting a human having sexual intercourse with an animal, regardless of the intent behind the post.

A photograph posted to an adult service depicting a sexual act threatening the life of the person involved, regardless of the intent behind the post.

A video posted to a social media site depicting rape, regardless of the intent behind the post.

Reasonably available information for user-to-user and search services:

The content suspected to be illegal content.

Content titles or descriptions of the content suspected to be illegal content.

Supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger.*

Reasonably available information for search services:

The content suspected to be illegal content.

Supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger.*

*A provider is not required to accept the opinions of a third party as to whether content is illegal content. Only a judgment of a UK court is binding on it in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

References

Legal annex: Section A11 of Annex 1.

Statute: Section 63 of the Criminal Justice and Immigration Act 2008.

Case law: Regina v Pin Chen Cheung [2009] EWCA Crim 2965; Regina v Baddiel [2016] EWCA Crim 474; Connolly v DPP [2007] EWHC 237 (Admin); R v Okoro (No. 3) [2018] EWCA Crim 1929.

Guidance on Content Harmful to Children: Section 2, 'Guidance on pornographic content'

Intimate image abuse

What is intimate image abuse?

1.27 'Intimate image abuse' relates to the non-consensual disclosure of, or threats to disclose, intimate images. There are multiple priority offences relating to intimate image abuse but they overlap with one another significantly. These priority offences are often referred to colloquially as 'revenge pornography', but the content need not be posted for revenge and are abusive content rather than legal pornography. We therefore do not use this term in this chapter.

1.28 In the following, 'Person A' refers to the person sharing the photograph or film, and 'Person B' refers to the person depicted in the photograph or film in an intimate state.

1.29 Service providers should consider whether the photograph or film has been disclosed:

a) without Person B's consent and
b) when Person A either (i) did not reasonably believe Person B consented; or (ii) is acting with the intention of causing Person B alarm, distress or humiliation.

What is a photograph or film?

1.30 A 'photograph' should be understood as any still image which is or appears to be a photograph, whether created by a camera, made by computer graphics or generated in any other way (for example, a still of a film). A 'film' should be understood as any moving image, including automated GIFs. Copies of photographs or films, or photographs or films which have been digitally altered, should be treated as the same as the original.

1.31 The inclusion of the 'appears to show' criteria of the offence means that manipulated images and videos such as deepfakes should be considered within the scope of this offence. Any photograph or video which appears to depict an intimate situation (see below) should be treated as a photograph or video actually depicting such a situation.

1.32 Data which is capable of being converted into an image or video, such as compressed image files, should be treated as equivalent to the image itself.

What is an 'intimate state' or 'intimate situation'?

1.33 A person should be understood to be in an 'intimate state' or 'intimate situation' if any of the following are true:

a) The person is engaging or participating in or present during (what a reasonable person would consider to be) a sexual act, which is not of a kind ordinarily done in public;
b) The person's genitals, buttocks, or breasts are:
    i) exposed,
    ii) covered only with underwear;
    iii) covered only by clothing that is wet or otherwise transparent; or
    iv) obscured by any means, other than by clothing that a person is wearing, where the obscured area is similar to or smaller than an area that would typically be covered by underwear worn to cover a person's genitals, buttocks or breasts (as the case may be). This includes instances where they are obscured by part of a person's body or by digital alteration.
c) The person in act of urination, defecation, or personal care associated with the person's urination, defecation or discharge.

1.34 Both 'upskirting' and 'downblousing' imagery are encompassed within the scope of this offence, in addition to photographs and videos shared by a victim with a previous partner, and intimate photographs and videos obtained through other means (such as hacking).

Consent, reasonable belief in consent and intent

1.35 Providers should look for identifier features which suggest lack of consent and either lack of reasonable belief in consent or intent to cause alarm, distress or humiliation. This may be evidenced by, for example:

a) an intimate image content report received from a user or affected person, or
b) another type of user report which suggests that the content has been posted non-consensually (absent evidence to the contrary, this should be taken as reasonable grounds to believe not only that there was no consent, but that Person A did not have reasonable belief in consent), or
c) contextual information accompanying the content which suggests that the photograph or video was posted for malicious reasons (for example, abusive descriptions of the person depicted, positioning the disclosure as an act of 'revenge'), or
d) contextual information which presents the image being shared as having been obtained through a 'hack' or 'leak'.

1.36 If the person portrayed consented to the disclosure the content is not illegal content.

Images that have been shared, forwarded or reposted

1.37 An image which a provider has reasonable grounds to infer was disclosed without consent (or without reasonable belief in consent) could then be shared, forwarded or reposted. In such cases, if there is an absence of evidence that the person who originally disclosed the image took appropriate steps to obtain consent from the subject of the image to disclose it, it is reasonable for a provider to infer that a person who subsequently shares, forwards or reposts the image does not have a reasonable belief in consent. The content should therefore be taken down.

Threats to disclose

1.38 In order for content to be considered illegal, it is not always necessary that a photograph or film depicting a person in an intimate state has been disclosed. It is also an offence to threaten to disclose a photograph or film which shows (or appears to show) a person in an intimate state. There must, however, be reasonable grounds to infer that the person making the threat 'intended' the person being threatened to fear that the threat would be carried out, or 'failed to think about' or was 'indifferent' as to whether this would be the case.

Relevant exemptions

1.39 Content is not illegal where there are reasonable grounds to infer that Person B was, when the photograph or film was taken or recorded, in a place to which the public or a section of the public had or were permitted to have access (whether freely or by paying a fee); Person B had no reasonable expectation of privacy from the photograph or film being taken or recorded; and Person B was in the intimate state voluntarily, or Person A reasonably believed that Person B was in the intimate state voluntarily. In practical terms, 'upskirting' and 'downblousing' photographs or videos are not covered by this exemption.

Defences

1.40 Person B also has a defence if they have a reasonable excuse. Some examples of likely reasonable excuses would be:

a) If they reasonably believed that the disclosure of the photograph or film was in the public interest. This may be the case where the disclosure is for journalistic purposes. However, providers should consider and may need to take UK legal advice on whether the right to journalistic freedom of expression outweighs Person B's right to privacy.

b) If they reasonably believed that the disclosure of the photograph or film was necessary for the purposes of the prevention, detection, investigation or prosecution of crime. This defence will not arise where the content is shared by a person who is not a member of the police or acting on police instructions.

Encouraging, assisting and conspiracy to intimate image abuse

1.41 As set out above, encouraging and assisting intimate image abuse, conspiracy to commit intimate image abuse and knowingly engaging together with someone else in pursuit of a common purpose to commit intimate image abuse are also priority offences. In all these cases, content will only be illegal content to the extent that the underlying offence of possession of intimate image abuse is sufficiently linked to the

UK – the question is whether the UK would prosecute the people involved. The rules which decide whether or not there is a sufficient link are very complicated and content moderators cannot be expected to understand them in detail. However, for the purposes of this guidance, content should be considered illegal if the person being encouraged or assisted, or with whom there is a conspiracy or a common purpose, is either British or located in the UK.

1.42 Encouraging could include words urging another person to carry out the offence. Assisting could include providing substantive help in carrying out the offence. There must either be intent to encourage/assist the offence, or belief that the offence will be committed. For conspiracy, there must be an agreement between two people and intent to carry out the offence. For a common purpose, both parties must knowingly share the purpose.

Risk assessment and intimate image abuse content

10.1 For the purposes of carrying out a risk assessment, providers should be aware that (priority) illegal content which amounts to intimate image abuse can take the form of videos or images (including those which have been digitally manipulated i.e. deepfakes), or links to these same videos or images.

10.2 Content amounting to these offences may be found on user-to-user services (including adult services, social media services, dating services, messaging services, video-sharing services, file-storage and file-sharing services, and discussion forums and chatrooms). Search services may also be used to search for and access such content, for example via video or image viewing facilities.

10.3 See the Register of Risk chapter titled 'Intimate image abuse.'

Usage examples

Photographs or video of nudity or a sexual act which is presented as having been obtained through a hack or leak.

Photographs or video of nudity or a sexual act which is presented as being disclosed without the consent of the person depicted.

A photograph that appears to have been taken down a person's shirt or blouse ('downblousing') or up their skirt ('upskirting') without consent.

A reshare or repost of a photograph or video which has already been judged to be illegal content by a provider.

Reasonably available information for user-to-user services

The content suspected to be illegal content.

Content titles or descriptions of the content suspected to be illegal content.

A report, including an intimate image content report, made by a user or affected person.

Supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger.*

Reasonably available information for search services

The content suspected to be illegal content.

A report, including an intimate image content report, made by a user or affected person.

Supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger.*

*A provider is not required to accept the opinions of a third party as to whether content is illegal content. Only a judgment of a UK court is binding on it in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

References

Legal annex: Section A11 of Annex 1.

Statute: Section 66(B) of the Sexual Offences Act 2003.

Notes: Section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 has not been considered separately in this guidance. For the purposes of making illegal content judgements, it overlaps in whole or in part with the Section 66(B) offence, which we have treated as the main offence for the purposes of threats above.

Cyberflashing

1.43 The Act creates the offence of intentionally sending a photograph or film of genitals for the purposes of causing alarm, distress or humiliation or for the purpose of obtaining sexual gratification. This offence is also known as 'cyberflashing' and is referred to as such for the purposes of this chapter.

1.44 While children can be victims of cyberflashing, the sexual nature of the offences in question mean that any content which involves a child and meets the threshold for an offence mentioned above will also automatically amount to a child sexual exploitation and abuse (CSEA) offence.[3]

1.45 This type of content will only appear on user-to-user services where inferences can be made about intention, purpose for sending and the intended recipient of the image or video. Cyberflashing content is unlikely to be found in a recognisable form in search results except where search results link through to content on a user-to-user (U2U) service. Therefore, the guidance below applies to user-to-user services only.

1.46 For more information on harms relating to cyberflashing, see the Register of Risk chapter titled 'Cyberflashing.'

1.47 Content will be illegal content where the following is true:

a) The content contains a 'photograph or film' of someone's genitals (the genitals in question do not need to be that of the sender); and
b) The content has been sent or shown by the sender to another person by any means, electronically or otherwise, or placed for a particular person to find; and

[3] In the case of cyberflashing, the content in question would likely amount to sexual communication with a child if sent by an adult. If sent by a child, the image itself would be classified as an indecent image of a child.

c) The sender has sent (etc.) the photograph or film with the intention of causing alarm, distress or humiliation on the part of the receiver, or
d) The sender has sent (etc.) the photograph for the purpose of obtaining sexual gratification, and been reckless as to whether by doing so the recipient may have experienced alarm, distress or humiliation.

1.48 The genitals being shown in the photograph or film do not need to be the genitals of the user sending the content. Genitals from, for example, a pornographic film or image would meet the definition of this type of content.

What is a 'photograph or film'?

1.49 A photograph should be understood as any still image which is or appears to be a photograph, whether created by a camera, made by computer graphics or generated in any other way (for example, a still of a film). A 'film' should be understood as any moving image, including automated GIFs. In Ofcom's view, AI-generated imagery, 'deepfakes' and other manipulated media which appear to be a photograph or a film are captured by this offence.

1.50 Copies of photographs or films, or data which can be converted to create a photograph or film (for example, a zipped file) should be treated as equivalent to the photograph or film itself.

1.51 Content which does not itself contain a photograph or film of genitals but which contains a URL which links to such content, will be illegal where the relevant state of mind requirement is made out.

State of mind

1.52 The state of mind requirement for this offence is intent to cause distress, alarm, or humiliation or, where the photograph or film is sent for the purpose of obtaining sexual gratification, recklessness as to whether alarm, distress or humiliation would be caused.

1.53 It will be reasonable for service providers to infer the required intent or recklessness where a user sends content depicting genitalia, unless:

a) there is evidence of consent from the user(s) receiving the photograph or film or
b) it is posted on a service where it is a commonly accepted part of the culture to send and receive intimate images without prior agreement.

1.54 Regardless of the type of service in which the content is sent, it is likely to be reasonable for service providers to infer intent or recklessness:

a) where there is explicit evidence of the intent behind sending the message, for example in the form of a comment on the face of the content or in surrounding contextual information (such as subsequent messages in a conversation), or
b) where the user sending the image has previously received warnings that sending such images is likely to cause distress.

Encouraging, assisting and conspiracy of the cyberflashing offence

1.55 Encouraging, assisting and conspiracy to commit the cyberflashing offence are also priority offences. In all these cases, content which amounts to the encouragement,

assistance, or conspiracy will only be illegal content to the extent that the offence which is being encouraged, assisted or conspired to is sufficiently linked to the UK – the question is whether the UK would prosecute the people involved. The rules which decide whether or not there is a sufficient link are very complicated and content moderators cannot be expected to understand them in detail. However, for the purposes of this guidance, content should be considered illegal if the person being encouraged or assisted, or with whom there is a conspiracy, is either British or located in the UK.

1.56 Encouraging could include words urging another person to carry out the offence. Assisting could include providing substantive help in carrying out the offence. There must either be intent to encourage/assist the offence, or belief that the offence will be committed. For conspiracy, there must be an agreement between two people and intent to carry out the offence.

Risk assessment and cyberflashing content

1.57 For the purposes of carrying out a risk assessment, providers should be aware that (priority) illegal content which amounts to the offence of cyberflashing can take the form of videos or images (including those which have been digitally manipulated i.e. deepfakes), or links to these same videos or images.

1.58 Content amounting to these offences may be found on user-to-user services (including social media services, messaging services, video-sharing services and dating services).

1.59 See the Register of Risk chapter titled ‘Cyberflashing.’

Usage examples

A photograph or video of a person’s genitals sent via a messaging app or via social media (for example, through a DM) to another user, where it appears to have been sent against the recipient’s wishes, and/or without warning or context.

A photograph or video of a person’s genitals, sent over a messaging app or other communications service to all users in a ‘meeting’ or group chat where it would not be commonly expected to appear.

A photograph or video of a person’s genitals, posted to a public comments section on a service where this is not a commonly accepted part of the service’s culture.

Reasonably available information for user-to-user services

The content suspected to be illegal content.

No more than three messages or posts immediately preceding content.

Supporting information provided by any complainant, including that which is provided by any person the provider considers to be a trusted flagger.*

*A provider is not required to accept the opinions of a third party as to whether content is illegal content. Only a judgment of a UK court is binding on it in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided

References

Legal annex: Section A11of Annex 1.

Statute: Section 66A of the Sexual Offences Act 2003.

A1. Adult image-based sexual offences

136. Sharing or threatening to share intimate photograph or film – s. 66B Sexual Offences Act 2003

Conduct (actus reus)

(1) P —

(a) **Shares** a **photograph** or **film** which shows, or appears to show, another person (B) in an **intimate state**; and

(b) B does not **consent** to the sharing of the **photograph** or **film**.

(2) P —

(a) **Shares** a **photograph** or **film** which shows, or appears to show, another person (B) in an **intimate state**; and

(b) B does not **consent** to the sharing of the **photograph** or **film**.

(3) P —

(a) **Shares** a **photograph** or **film** which shows, or appears to show, another person (B) in an **intimate state**; and

(b) B does not **consent** to the sharing of the **photograph** or **film**.

(4) P —

(a) Threatens to **share** a **photograph** or **film** which shows, or appears to show, another person (B) in an **intimate state**.

State of mind (mens rea)

In the case of (1): P intends to **share** the **photograph** or **film** and does not **reasonably believe** that B **consents**.

In the case of (2): P intends to **share** the **photograph** or **film** and does so with the intention of causing B alarm, distress or humiliation.

In the case of (3): P intends to **share** the **photograph** or **film** for the purpose of P or another person obtaining sexual gratification, and P does not **reasonably believe** that B **consents**.

In the case of (4): P carries out the threat with the intention that B or another person who knows B will fear that the threat will be carried out, or is **reckless** as to whether B or another person who knows B will fear that the threat will be carried out.

Defences

In the case of (1):

(a) It is a defence for P to prove that they had a reasonable excuse for sharing the **photograph** or **film** (s.66B(8) of the Sexual Offences Act 2003).

(b) P does not commit an offence if:

(i) B is a person under 16;

(ii) B lacks, or P reasonably believes that B lacks, capacity to **consent** to the sharing of the photograph or film; and

(iii) the **photograph** or **film** is shared with a healthcare professional acting in that capacity, or otherwise in connection with the care or treatment of B by a healthcare professional

(s.66C(4) of the Sexual Offences Act 2003).

(c) P does not commit an offence if the **photograph** or **film** shows, or appears to show, a child in an **intimate state** and the **photograph** or **film** is of a kind ordinarily shared between family and friends (s.66C(5) of the Sexual Offences Act 2003).

In the case of (1), (2) and (3):

(a) P does not commit an offence if the **photograph** or **film**:

(i) was taken or recorded, or P reasonably believes that it was taken or recorded, in a place to which the public or a section of the public had or were permitted to have access (whether on payment or otherwise);

(ii) B had no **reasonable expectation of privacy** from the **photograph** or **film** being taken or recorded; and

(iii) B was, or P reasonably believes that B was, in the **intimate state** voluntarily

(s.66C(1) of the Sexual Offences Act 2003).

(b) P does not commit an offence if:

(i) the **photograph** or **film** had, or P reasonably believes that the **photograph** or **film** had, been previously publicly shared; and

(ii) B had, or P reasonably believes that B had, **consented** to the previous sharing

(s.66C(3) of the Sexual Offences Act 2003).

In the case of (4): P does not commit an offence if, by reason of any of the matters set out above, they would not commit an offence under cases (1), (2) or (3) by sharing the **photograph** or **film** in the circumstances conveyed by the threat (s.66C(6) of the Sexual Offences Act 2003).

Definitions and interpretations

Consent: Includes general consent covering the particular act of **sharing** as well as specific consent to the particular act of **sharing** (s.66B(6)(a) and s.66D(10) of the Sexual Offences Act 2003). Where the defendant intentionally deceived the complainant as to the nature or purpose of the relevant act, or the defendant intentionally induced the complainant to consent by impersonating a person known personally to the complainant, it is conclusively presumed that the complainant did not consent and the defendant did not reasonably believe that the complainant consented (s.66B(5A) of the Sexual Offences Act 2003.

Exposed: A reference to all or part of a person's "exposed" genitals, buttocks or breasts includes —

(a) A reference to all or part of the person's genitals, buttocks or breasts visible through wet or otherwise transparent clothing;

(b) the case where all or part of the person's genitals, buttocks or breasts would be exposed but for the fact that they are covered only with underwear; and

(c) the case where all or part of the person's genitals, buttocks or breasts would be exposed but for the fact that they are **obscured**, provided that the area obscured is similar to or smaller than an area that would typically be covered by underwear worn to cover a person's genitals, buttocks or breasts (as the case may be)

(s.66D(6) of the Sexual Offences Act 2003).

Film: A moving image. References to a film also include—

(a) an image, whether made or altered by computer graphics or in any other way, which appears to be a film;

(b) a copy of a film or image within paragraph (a); and

(c) data stored by any means which is capable of conversion into a film or image within paragraph (a)

(ss.66A(4), (5) and 66D(4) of the Sexual Offences Act 2003).

Intimate state: Except where a **photograph** or **film** shows or appears to show something other than breastfeeding (which includes the rearranging of clothing in the course of preparing to breastfeed or having just finished breastfeeding) that is of a kind ordinarily seen in public, a **photograph** or **film** "shows, or appears to show, another person in an intimate state" if it shows or appears to show—

(a) the person participating or engaging in an act which a reasonable person would consider to be a sexual act;

(b) the person doing a thing which a reasonable person would consider to be sexual;

(c) all or part of the person's **exposed** genitals, buttocks or breasts;

(d) the person in an act of urination or defecation; or

(e) the person carrying out an act of personal care associated with the person's urination, defecation or genital or anal discharge

(s.66D(5), (8) and (9) of the Sexual Offences Act 2003).

Obscured: Means obscured by any means, other than by clothing that a person is wearing, including, in particular, by an object, by part of a person's body or by digital alteration (s.66D(7) of the Sexual Offences Act 2003).

Photograph: Includes the negative as well as the positive version. References to a photograph also include—

(a) an image, whether made or altered by computer graphics or in any other way, which appears to be a film;

(b) a copy of a film or image within paragraph (a); and

(c) data stored by any means which is capable of conversion into a film or image within paragraph (a)

(ss.66A(3), (5) and 66D(4) of the Sexual Offences Act 2003).

Reasonable belief: Whether a belief is reasonable is to be determined having regard to all the circumstances including any steps P has taken to ascertain whether B consents (s.66B(6)(b) of the Sexual Offences Act 2003).

Reasonable expectation of privacy: Whether a person had a reasonable expectation of privacy from a **photograph** or **film** being taken is to be determined by reference to the circumstances that the person sharing the **photograph** or **film** reasonably believes to have existed at the time the **photograph** or **film** was taken (s.66C(2) of the Sexual Offences Act 2003).

Reckless: See 'General Interpretation.'

Share: A person "shares" something if the person, by any means, gives or shows it to another person or makes it available to another person (s.66D(2) of the Sexual Offences Act 2003).

Further notes

- In the case of the offence at (4), it is not necessary to prove —

  (a) that the photograph or film mentioned in the threat exists; or

  (b) if it does exist, that it is in fact a photograph or film which shows or appears to show a person in an intimate state

  (s.66B(7) of the Sexual Offences Act 2003).

- A provider of an internet service by means of which a **photograph** or **film** is **shared** is not to be regarded as a person who **shares** it, or as a person with whom it is shared (s.66D(3) of the Sexual Offences Act 2003).