Harmful content (KCSIE 2026) Summary

Overview

Children can encounter harmful online content across social media, apps, livestreams, games and messaging platforms. Harm may arise from sexual content, violent/distressing content, online hate, harmful challenges/hoaxes, value-based extremist content, biased content (self-harm, suicide, eating disorders), edited/AI-generated content, mis/disinformation, and dark web risks. All harmful content can impact a child's wellbeing, behaviour, safety and development.

Staff must consider **contextual safeguarding**, SEND vulnerabilities, and wider environmental factors that may increase risk.

Key Types of Harmful Content

Sexual Content / Pornography Includes suggestive messages, legal adult content, illegal violent pornography, and AI-generated sexual imagery (deepfakes, nudification). All sexual images of children — real, altered or AI-generated — are illegal. **Follow:** HSB Policy + Nudes & Semi-Nudes Policy.	**Violent, Distressing or Aggressive Content** Includes fights, dares, animal abuse, torture, extreme violence. Can cause fear, confusion, desensitisation or imitation, especially for SEND pupils.
Online Hate Content Includes prejudiced, derogatory or threatening content targeting protected characteristics. May constitute hate crime or extremist behaviour. **Follow:** Prevent Policy.	**Harmful Online Challenges & Hoaxes** Hoaxes spread false, distressing information; challenges may be dangerous or life-threatening. Staff must not name hoaxes/challenges. DSLs assess risk case-by-case.
Value-Based Extremist Content Includes terrorist or extremist material shared via websites, forums or messaging apps. **Report:** Police or GOV.UK extremism reporting. **Follow:** Prevent Policy.	**Biased Content** Includes self-harm/suicide forums, pro-ana/pro-mia content (anorexia and bulimia) 'bonespiration' and harmful ideologies. Normalises unsafe behaviours.
Edited Content / Generative AI Filters, editing tools and AI manipulation can distort body image, create deepfakes, or be used for bullying/harassment. **Follow:** AI risks & Online Safety Policies.	**Misinformation & Disinformation** False or misleading content spread intentionally or unintentionally. Algorithms amplify sensational or conspiratorial content. Children may struggle to identify reliable information.
Dark Web Risks Accessed via encrypted browsers (.onion). Associated with illegal downloads, extreme content, exploitation, drugs and criminal activity. **Immediate DSL referral required.**	

Staff Responsibilities

- Maintain an attitude of *"it could happen here."*
- **Do not view, download, save or investigate** harmful content.
- Report all concerns **immediately to the DSL** and **log on CPOMS**. Or whistle blow to Head if concern is with staff use or exposure
- Avoid naming harmful challenges or hoaxes.
- Offer reassurance and ensure pupils know how to access support.
- Consider contextual safeguarding, SEND vulnerabilities and links to: **HSB**, **Nudes & Semi-Nudes**, **Prevent**, **Online Safety**, **AI**, **Children at Greater Risk of Harm**.

- Staff use of AI tools restricted to Trust-agreed Copilot to minimise risk

DSL Responsibilities

- Lead risk assessment and determine thresholds for Police, ICS, Prevent or Online Safety escalation.
- Ensure clear CPOMS recording of decisions, actions and rationale.
- Prevent further exposure to harmful content; avoid naming hoaxes/challenges.
- Provide tailored support and education for affected pupils.
- Monitor patterns, liaise with external agencies, and review filtering/monitoring systems.
- Cross-reference incidents with **HSB**, **Nudes & Semi-Nudes**, **Prevent**, **AI**, and **Safeguarding & Child Protection** policies.

Support & Education for Pupils

- Help children process what they have seen and ask questions safely.
- Teach blocking/reporting tools and safe navigation strategies.
- Promote media literacy, critical thinking and healthy online habits.
- Encourage reviewing feeds, muting/unfollowing harmful accounts, and understanding edited/curated content.
- Ensure pupils know trusted adults and support services (e.g., Childline).

Policy document for: **Harmful content**
Updated: Autumn 2026

This policy forms part of the Trust Safeguarding and Child Protection policy and reflects the latest KCSIE guidance. Keeping children safe in education 2026 (comes into force from 1 September 2026) ***All staff must read Part 1 as a minimum.***

This policy reflects KCSIE 2026 (Part 2 and Annex B) and the Trust Online Safety Framework

Harmful content

Harm is defined as ill-treatment or the impairment of health or development including, for example, impairment suffered from seeing or hearing the ill-treatment of another. This includes sexual and emotional abuse. Online content can harm from sexual contents or pornography, violent/distressing/aggressive content, value based content or biased content.

Linked policies

- Harmful Sexual behaviour (HSB) policy
- Nudes and semi-nudes
- Prevent
- Online safety
- Cyber crime
- Child protection and safeguarding

Sexual content and pornography

Children may encounter sexual content online ranging from suggestive messages and legal adult material to illegal violent pornography. Such content can appear across social media, apps, livestreams and games — both intentionally and accidentally — through searches, adverts, shared links or older users' devices. Exposure can cause confusion, distress, desensitisation or imitation of harmful behaviours.

All concerns or disclosures must be reported to the DSL, recorded on CPOMS, and managed under the **Safeguarding and Child Protection Policy**.

Where sexual content involves coercion, sharing of sexual images, or AI-generated sexual imagery, staff must follow the **Harmful Sexual Behaviour (HSB) Policy** and the **Nudes & Semi-Nudes Policy**, as these outline statutory responses under **KCSIE 2026 Part Five**. These policies clarify that all sexual images of children — whether real, altered or AI-generated — are illegal and must be treated as child sexual abuse material.

AI-Generated Sexual Content (Deepfakes, Nudification and Altered Images)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Microsoft CoPilot. We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully or harass others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Additionally, many platforms have in-app filters or editing tools to help users to alter images or videos. Children enjoy these as they can be used for fun. However, when filters or tools are used to enhance or alter physical features, this can lead young people to compare themselves to others online and to have an unrealistic view of acceptable beauty standards. It's not always easy to recognise when someone is using a filter, for example there are tools available that enable you to edit your appearance during a livestream or video call.

The impact filters and editing tools can have include the following:

- They can affect young people's self-esteem and body image;
- Young people may feel pressure to post certain images to 'fit in';
- They can affect young people's overall well-being;
- Young people may feel disappointment or embarrassment if they don't get enough 'likes' or comments;

Seeing a friend, influencer or celebrity posting an edited image or video online can also negatively affect a young person's self-esteem and put pressure on them to post certain types of images. Children and young people need to know that often people will only share certain aspects of their lives which can lead followers to believe that they live a perfect life. Many influencers are paid to create aspiring content as a way to encourage people to buy products and make money.

Artificial intelligence tools can create sexualised images, videos or audio of children that appear real, including deepfakes, nudification apps and digitally altered sexual content. KCSIE 2026 is clear that **AI-generated sexual images of children are illegal**, regardless of whether a real child was involved, and must be treated as child sexual abuse material.

AI-generated bullying or impersonation must be treated as online sexual harm if sexualised. See **Harmful Sexual Behaviour (HSB) policy** and **Online Safety policy.**

Staff must not view, save, copy or investigate such content. Any concerns or disclosures must be reported immediately to the **DSL**, logged on CPOMS, and managed in line with the **Harmful Sexual Behaviour (HSB) Policy** and the **Nudes & Semi-Nudes Policy**, which set out the statutory response, risk assessment process and referral pathways. AI-generated sexual content involving coercion, blackmail, harassment or sharing must always be treated as a safeguarding incident and may constitute a criminal offence.

See also the **Generative AI and safeguarding risks** policy.

Violent, distressing or aggressive content

Violent or distressing content can be accessed over a variety of online platforms such as games, music, social media posts and videos. The range of content may include children and young people sharing posts of themselves fighting or conducting violence for dares, to disturbing images such as abuse or torture of animals. The impact of viewing such images can evoke a range of emotions such as confusion, worry, fear for themselves or others and may evoke changes in behaviour. Worryingly, viewing such images for some children, especially those with SEND, may lead to desensitisation, where they see the acts and images as harmless or 'a bit of fun'. This can lead them to replicate the behaviour viewed.

Staff must consider contextual safeguarding and SEND vulnerabilities when assessing risk.

Online hate & extremist content

The term 'online hate' refers to the posting and sharing of hateful and/or prejudiced content on any online platform. Usually targeted against an individual, group or community, such content may be

derogatory, demonising and dehumanising and often includes threats, harmful insinuations, identity-focused insults, disparaging terms and allegations designed to cause reputational damage.

If such content is hostile towards a person's race, religion, disability, sexual orientation or gender identity, it could also be viewed under the law as hate speech.

In line with statutory guidance on the recording of so-called non-crime hate incidents, incidents which are trivial or irrational and do not amount to a criminal offence, the police will only record non-crime hate incidents when it is absolutely necessary and proportionate and not simply because someone is offended

Online hate can be expressed through many types of media including text, images, videos and audio and often a combination of types are used to:

- Send malicious communications designed to cause distress, fear and/or anxiety;
- Cause harassment;
- Carry out cyberbullying;
- Undertake cyberstalking;
- Incite hatred;
- Incite others to commit violent acts

Any such concerns or disclosures should be reported to a DSL, logged on CPOMS and action taken in line with the **safeguarding and child protection** policy. A referral under Prevent may also be needed if extremist indicators are present.

Value based content

Terror and extremist content can be found on specific websites and forums online and such material can then be shared through messaging apps. Such content is illegal and if found must be reported on Report online material promoting terrorism or extremism - GOV.UK (www.gov.uk) or directly to the Police.

Seeing such content can be very scary, confusing or worrying for children, but it could also spark their interest or curiosity, leading to a risk of radicalisation.

Staff must not download or share extremist material for training or awareness in line with Prevent guidance.

Radicalisation

If a member of staff has a concern about a child then they should report it immediately to a DSL and log the concern on CPOMS. If there is an immediate risk of harm, the staff member should contact the Police immediately.

See **Prevent** policy for full details.

Harmful online challenges and online hoaxes

A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

Any member of staff who identifies a potential hoax or harmful challenge which may be putting children at risk should report this on CPOMS and flag the DSL team. The DSL team will undertake a case by case assessment to consider if this is a national risk, localised or within the school. Rapid action may prevent

the hoax or challenge becoming viral and impacting more children. Decisions about whether to notify parents will be informed by the case assessment.

The DSLs make use of the Kent Education Safeguarding Service and the Professional Online Safety Helpline on https://www.saferinternet.org.uk/helpline/professionals-online-safety-helpline

Is it an online hoax?

A hoax is a deliberate lie designed to seem truthful. The internet and social media provide a perfect platform for hoaxes, especially hoaxes about challenges or trends that are said to be harmful to children and young people to be spread quickly.

The DSLs will carefully consider if a challenge or scare story is a hoax. It is important that such hoaxes are not referred to by name to avoid children searching for them and joining in. Concerns are often fuelled by unhelpful publicity, usually generated on social media, and may not be based on confirmed or factual occurrences or any real risk to children and young people. There have been examples of hoaxes where much of the content was created by those responding to the story being reported, needlessly increasing children and young people's exposure to distressing content.

Evidence from Childline shows that, following viral online hoaxes, children and young people often seek support after witnessing harmful and distressing content that has been highlighted, or directly shown to them (often with the best of intentions), by parents, carers, schools and other bodies

Is it a real online challenge that might cause harm to children and young people?

An online challenge will generally involve users recording themselves taking a challenge and then distributing the resulting video through social media sites, often inspiring or daring others to repeat the challenge. Whilst many will be safe and fun, others can be potentially harmful and even life threatening.

Where the DSLs are confident children and young people are aware of, and engaged in, a real challenge that may be putting them at risk of harm, it will be directly addressed. This may be through focussed support to a particular age group or individual children at risk. Remember, even with real challenges, many children and young people may not have seen it and may not be aware of it. It is important that such challenges are not referred to by name to avoid children searching for them and joining in.

Key questions used to evaluate the risk are:

- is it factual?
- is it proportional to the actual (or perceived) risk?
- is it helpful?
- is it age and stage of development appropriate?
- is it supportive?

- The incident will be recorded on CPOMS (and the online challenge named) and the DSLs may share information with parents/carers from National Online Safety about keeping children safe in a particular social media environment to support.
- See also the **child protection and safeguarding** policy and **online safety** policy

Biased content

The online world contains an enormous amount of information which can be used to learn new things or to verify facts. However, it is important for staff and children to remember that not all information is true/factual and may be biased to be incorrect or wrong. It could also be harmful when it shares messages/ideologies around self harm/suicide, eating disorders etc.

Self harm/suicide

There is a growing concern that young people are using the internet to join groups or forums which support and encourage self harm or suicidal behaviours and thoughts, including pictures and videos. This then 'normalises' the behaviour and thoughts. This is a significant risk for young people.

Any such concerns or disclosures should be reported to a DSL, logged on CPOMS and action taken in line with the **safeguarding and child protection** policy.

Eating disorder content

There are many forums and social media platforms which share positive, supportive content which promote healthy eating and trusted health information. However there are harmful sites which promote anorexia (pro-ana) or bulimia (pro-mia) where users shares '*thinspiration'* with tips and images for not eating and avoiding weight gain. This content encourages people to be thin, whereas '*bonespiration'* advocates extreme thinness with protrusion of bones.

These online platforms and forums may initially look like support, they contain very harmful content.

For more information:

- The Dangers of Pro-Ana and Pro-Mia Content | Seeds of Hope
- Understanding "Proana": What It Is & Why It's Harmful | Aster Springs
- The Dangers of Pro-Ana and Pro-Mia - Beat

This is a growing issue with young men and boys although is seen a predominately female issue. Staff should be aware that we must be aware of the impact on the boys in school.

Pro-ana and Pro-Mia content

These are groups which are linked to anorexia and bulimia. Whilst the internet has groups which offer support for those in recovery, these groups promote or romanticise behaviours and mindsets linked to anorexia and bulemia

Looksmaxxing

There is a growing online/social media trend pushing boys towards extreme body obsession, misogyny and self harm. This can be delivered through social media influencers, masculinity coaches, misogynistic content being pushed on platforms (when it is not searched for) and wellness brands which monetise anxiety, insecurity and isolation whilst sowing intolerance, bigotry and misogyny.

See Centre for Young Lives | Don't blame life, blame your face - Safeguarding Board for Northern Ireland

Any such concerns or disclosures should be reported to a DSL, logged on CPOMS and action taken in line with the **safeguarding and child protection** policy.

Misinformation and disinformation

- *Misinformation* is false or misleading information that is unwittingly shared.
- *Disinformation* is deliberately created and distributed with the intent to deceive or harm.

Together they range from satire and parody to dangerous conspiracy theories and include fake news. Misinformation and disinformation (mis/disinformation) online is an ongoing issue as it's rapid spread

online affects everyone and, as digital users, it is very much a part of children's lives. Social media provides the vehicle for it to spread farther, faster, and deeper. Divisive issues, such as immigration, gender politics and equality, and vaccination are common subjects.

Whilst also spread by people, algorithms are a key part of the mis/disinformation flow. Algorithms drive personalised news feeds and curate search results, content, and friend recommendations by tracking user behaviour. Algorithms sometimes promote misleading, sensationalist and conspiratorial content over factual information, and can be key vectors in amplifying the spread of mis/disinformation.

Children are particularly vulnerable to the risks of mis/disinformation because of their evolving capacities, where they cannot always distinguish between reliable and unreliable information. As a result, not only can they be harmed by mis/disinformation but they may also spread it amongst their peers. Even very young children or those without access to social media networks may be exposed to mis/disinformation through their interactions with peers, parents, caregivers and educators.

Any such concerns or disclosures should be reported to a DSL, logged on CPOMS and action taken in line with the **safeguarding and child protection** policy.

The dark web

The dark web is a part of the internet which offers the person accessing it and the websites they view, total anonymity. This is only possible using a special browser which encodes all the activity being undertaken and puts this through multiple layers of encryption – known as 'onion skin routing'. Common browsers such as Google, Chrome and Bing cannot access the dark web. However the anonymity this offers means it is exploited by criminals and poses a safeguarding risk for children.

Some children are tempted to find out how to access the dark web. The most common way of accessing this is through online gaming and illegal download sites. The games on these sites are likely to be extreme in their depiction of violence and sexual content and may be illegal and disturbing. Many of the files downloaded from illegal download sites are likely to be impregnated with highly exploitative viruses.

Use of anything from the dark web is extremely unwise as they have most likely been provided by dangerous and unscrupulous criminal elements. Such sites are likely to be 'honeytraps' set by criminal or paedophile gangs in order to harvest information used to groom or gain leverage over users to extort and blackmail them either for money or sexual exploitation.
Another possible draw of the dark web is by those wishing to obtain illegal drugs. There are reportedly factories in the Far East producing illegal drugs on an industrial scale. Much of their merchandise is sold via the dark web and available via mail order. Many of these drugs are highly addictive and extremely potent and dangerous. Use of these drugs have been fatal in a high proportion of cases.

It is difficult to justify why most people in the UK would access the dark web for legitimate purposes. If you become aware of a pupil accessing the dark web, especially websites with the suffix '.onion' then this should be immediately reported to a DSL.

Staff responsibilities

- Staff must maintain an attitude of *"it could happen here"* and act immediately on any concern involving harmful online content.
- Staff must **not investigate, view, download or share** sexual, violent, extremist or distressing material.
- All concerns must be **reported to the DSL, logged on CPOMS**, and managed in line with the **Safeguarding and Child Protection** Policy.
- Staff must offer reassurance to children, avoid showing or naming harmful content, and ensure pupils know how to access support.

- Staff must remain alert to contextual safeguarding factors, SEND vulnerabilities, and any indicators that content may link to **HSB**, **Nudes & Semi-Nudes**, **Prevent**, or **Online Safety** risks.

DSL responsibilities

- DSLs must lead the risk assessment, determine whether content indicates sexual harm, exploitation, coercion, radicalisation, or wider contextual risks, and take immediate action where required.
- DSLs must decide whether concerns meet thresholds for Police, ICS, Prevent, or Online Safety escalation, and ensure all decisions are recorded clearly on CPOMS.
- DSLs must avoid naming harmful challenges or hoaxes, prevent further exposure, and coordinate tailored support for affected pupils.
- DSLs must monitor patterns, liaise with external agencies, ensure filtering/monitoring systems are effective, and cross-reference incidents with the **HSB Policy**, **Nudes & Semi-Nudes Policy**, **Prevent Policy**, and **AI/Online Safety Policy**.

Support and education for children having viewed harmful content

In addition to reporting concerns, which are followed up through the child protection and safeguarding policy, children must be offered tailored support.

This support will be personalised to the child and the incident/impact, but should:

- Help them to understand and process what they have seen
- Help the child to ask questions or share their fears
- Help the child to learn how to block or report content
- Help the child to know how they can safely navigate and search the internet without fears of seeing similar content again
- Ensure the child knows how to access help if they see harmful content again
- Offer support for underlying issues

Age and stage appropriate education is vital to support children so that they can learn how to navigate the online world more safely. This will include:

- Talking to children about editing tools, where they see content and how this makes them feel;
- Reminding children that what we see online is often a highlights reel. This can even be the case when someone is sharing something sad. Often the day-to-day realities are not portrayed online;
- Exploring options to mute or unfollow accounts;
- Encouraging children to regularly review their feeds and unfollow / mute / block anyone who doesn't make them feel good about themselves;
- Exploring tools that hide 'likes' from other accounts;
- Reminding them that they always have someone who they can talk to and trust if they're feeling low or worried about something;
- Making other services known and available e.g. Childline and/or bespoke local services
- Critical thinking education and media literacy to help children recognise misinformation
- See the PSHE/SRE curriculum and Education for a Connected World framework

Staff must remain aware that SEND children are particularly vulnerable online. See the **Children at greater risk of harm** policy for more details.

DSL flowchart

