Department for Digital, Culture, Media & Sport

[redacted]
Minister of State in the Department for
Digital, Culture, Media and Sport
100 Parliament Street
London SW1A 2BQ

Ms Rachel Knight
HM Coroner
South Wales Central

18 September 2026

Dear Ms Knight,

Thank you for your Regulation 28 Report to Prevent Future Deaths dated 28 July 2026, regarding the tragic death of Cai Rhys Davies. As the Minister responsible for the Online Safety Act and online harms more broadly, I am responding on behalf of the Department for Digital, Culture, Media and Sport and the Department for Education (England), having both received your Prevention of Future Deaths Report.

First and foremost, I want to extend my deepest sympathies to Cai's family and friends. Every loss of life is a tragedy, but it is especially heartbreaking when it involves a young person with so much of their future ahead of them. The circumstances surrounding Cai's death are profoundly troubling, and I am grateful to you for drawing these matters to my attention.

This response addresses your concerns that fall within our respective remits. While the Online Safety Act applies across the United Kingdom, the Department for Education's contribution relates to education policy in England, reflecting that education is a devolved matter. We understand that Welsh Ministers will respond separately on matters within their devolved responsibilities. In preparing this response, my officials have also made enquiries with the Home Office to ensure we adequately address your concerns. Additionally, while we recognise that Cai was over the age of eighteen, we have included information on the child safety provisions in the Online Safety Act and wider Government action to protect children, reflecting that children are particularly vulnerable to online harms.

Non-consensual intimate imagery

The '*Freedom from Violence and Abuse: a cross-government strategy',* published in December 2025, sets out concrete actions to prevent violence and abuse, pursue perpetrators, and support victims. This includes a commitment to explore routes to ensure that intimate images that are taken, created or shared without consent are removed online. In February 2026, it became a criminal offence under Sexual Offences Act 2003 to create, or request the creation, of an intimate image of another person without consent. The government is introducing further protections against intimate image abuse via the Crime and Policing Act, which received Royal Assent on 29 April 2026. This includes an obligation for online platforms to have systems and processes in place to remove reported non-consensual intimate image abuse (NCII) content within 48 hours, and new criminal

offences of taking an intimate image without consent, and copying or screenshotting an intimate image without consent. In May 2026, Ofcom published amendments to the Online Safety Act's Illegal Content Codes of Practice recommending that certain higher-risk services use hash-matching technologies, or equivalent tools, to proactively detect and prevent the re-upload of known non-consensual intimate images (NCII). The update is expected to take effect this Autumn. The Home Office also provides funding to the Revenge Porn Helpline, who offer support and advice to victims of intimate image abuse, including assisting in the removal of NCII content online, and engages with law enforcement and other stakeholders to improve the response to NCII and raise awareness.

The government committed to making it impossible for children in the UK to take, share or view nude images. To deliver this commitment, the government announced a programme of engagement with technology companies so that they activate built-in safety features or implement technical solutions on smartphones and tablets that can prevent under 18s from creating and sharing nude images. Following this engagement, on 8 September, the Secretary of State for the Department for Digital, Culture, Media and Sport announced that the government will introduce primary legislation to require major tech companies to build in stronger device-level protections for children. These measures are intended to reduce opportunities for predators to exploit and abuse young people online, including through sextortion and other forms of image-based abuse.

Financially motivated sexual extortion

The government remains committed to tackling all forms of child sexual abuse, including Financially-Motivated Sexual Extortion (FMSE). FMSE involves offenders threatening to share sexually explicit or intimate material of the victim, unless financial demands are met. Victims of FMSE can be of any age and gender, although the primary targets amongst children are understood to be boys. The government is strengthening the UK's response to online child sexual exploitation through investment in the NCA, GCHQ, the Undercover Online Network and the Tackling Organised Exploitation Programme, ensuring law enforcement has the capabilities to identify and disrupt the highest-harm and most technically sophisticated offenders while engaging sensitively with children, victims and survivors. Alongside enforcement activity, NCA CEOP provides education, training and resources to help children, families and professionals stay safe online. This includes a recent alert sent to schools in England and Wales, raising awareness on FMSE and updated online blackmail resources for young people. Children can also access the Report Remove service, delivered by Childline and the Internet Watch Foundation (IWF), which enables them to confidentially report and remove sexual images of themselves from the internet. In 2024, reports to Report Remove increased by 44%, with 1,142 children seeking support to remove intimate images shared online without consent.

The Online Safety Act

The Online Safety Act ('the Act') received Royal Assent in October 2023. The Act lays the foundation for strong protections against illegal content for all users and harmful material for children. This includes offences relating to intimate image abuse and encouraging or assisting suicide, which are priority offences under the Act. This means that services must have systems and processes in place to prevent UK users from encountering this content. The government is committed to working with Ofcom, the independent regulator, to ensure it is implemented quickly and effectively.

Ofcom has robust enforcement powers and is promoting strong compliance with the Act. Ofcom is able to issue substantial fines to non-compliant services (up to 10% of qualifying worldwide revenue or £18 million, whichever is greater), or apply to the courts for business disruption measures that require third parties to withdraw their services from, or restrict access to, non-compliant services in the UK. Ofcom can take enforcement action against any company that provides services to UK users, wherever they are located. This is necessary given the global nature of the online world.

Ofcom's Illegal Content Codes of Practice sets out measures services can take to comply with their illegal content duties under the Act, including content moderation and user reporting and complaints mechanisms. The government and Ofcom continue to strengthen this framework. Ofcom has consulted on a wider package of Additional Safety Measures, including proposals to strengthen protections against intimate image abuse and suicide and self-harm content, and expects to publish its final decisions this Autumn.

The strongest protections in the Act are for children. Services are required to employ highly effective age assurance to prevent children from encountering the most harmful types of content. This includes pornographic content, and content which encourages, promotes or provides instructions for self-harm, suicide or eating disorders. Services are also required to provide age-appropriate experiences and protect children from other types of harmful legal content, including bullying, abusive and violent content.

In April 2025, Ofcom published their Child Safety Codes, setting out measures companies should take if their services pose a risk of exposing children to harmful content. These include employing highly effective age assurance technology; requirements for platforms to change their algorithms to filter out harmful content for children; and provision of effective systems so parents and children can easily report and get responses about harmful online content. More recently, the government announced further protections for children online, including preventing social media from offering their services to under-16s and access to harmful functions such as stranger communication and live streaming on a wider range of online services.

Department for Education (DfE), England

Keeping children safe in education (KCSIE) is statutory guidance that all schools and colleges must have regard to when carrying out their duties to safeguard and promote the welfare of children. KCSIE is kept under regular review to ensure it is meeting the needs of schools and colleges, and on 1 September DfE published strengthened guidance on issues central to our children's safety such as grooming and exploitation.

The updated statutory guidance for relationships, sex and health education, which schools are now required to teach, is clear that secondary aged pupils should learn about sextortion as part of teaching about online safety and harms. Pupils should understand the law relating to online sexual harassment and online sexual abuse, including grooming and sextortion. Pupils should learn about risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been affected. The previous statutory guidance, taught in schools since September 2020, already required pupils to be taught how to keep safe online, including recognising risks, harmful content and contact, and how and to whom to report issues.

DCMS UK-wide media literacy initiatives

The government recognises the importance of equipping children and young people with the knowledge and skills to navigate the online world safely. In March 2026, the government published *A Safe, Informed Digital Nation*, its cross-government Media Literacy Action Plan, which includes action to help people identify potentially harmful or deceptive online approaches and seek support when needed. In addition, the government has launched the Kids Online Safety Hub, providing carers with trusted advice and practical tools to support children's critical thinking, resilience and safer online habits, and has committed to expanding this support following the *Growing up in the Online World* consultation.

I would like to thank you again for bringing these matters to my attention. As the minister responsible, the Government and I, are fully committed to making the online world as safe as it can be for everyone, especially children and young people. Should you have any further queries or concerns regarding the actions set out above, the relevant government departments would be best placed to respond.

Yours sincerely,





Minister of State in the Department for Digital, Culture, Media and Sport