TAXONOMY ANNEX: POLICY MAPPING

This annex sets out the identified instruments underpinning the policy analysis in the harms taxonomy. The mapping covers 210 identified laws, policy frameworks and strategies: 75 in the UK, 56 in Canada and 70 in Ireland (including EU instruments that apply in Ireland as a Member State), as well as 7 in Australia and 2 in New Zealand (with a narrower comparative digital policy focus). Regulators and other public bodies are highlighted where relevant but are not counted as instruments. Findings and ratings reflect the information available on 11 November 2026.

Key instruments in the UK

The Online Safety Act 2023 (OSA) applies across the UK, but criminal law is partly devolved and individual offences differ in territorial coverage. The mapped frameworks apply mainly to England, or England and Wales. Scotland, Wales and Northern Ireland have separate, often overlapping, criminal safeguarding and health frameworks, which are noted where relevant.

Criminal law

Criminal law makes up the foundation and largest group of relevant UK frameworks to address men's and boys' online harms. Long-standing offences are largely technology and gender-neutral and apply only once a harm has occurred. For online safety purposes, these usually apply if the act of posting, sharing, threatening or dealing with content amounts to an offence (rather than whether the content merely depicts unlawful conduct).

The Protection from Harassment Act 1997 (England, Wales and Scotland) criminalises harassment. The Malicious Communications Act 1988 and section 127 of the Communications Act 2003 cover threatening and abusive communications. Part 10 of the OSA replaced parts of both with new false and threatening communications offences. Additionally, it added offences of cyberflashing and of encouraging or assisting serious self-harm.

Under the Theft Act 1968 (England and Wales), blackmail is the main offence for financial sexual extortion. Scotland relies on the common law offence of extortion. The Fraud Act 2006 covers online scams through false representation, while the Computer Misuse Act 1990 covers hacking and account takeover. Money laundering offences under the Proceeds of Crime Act 2002 apply to 'money mules' who allow their accounts to be used to move criminal funds.

The Public Order Act 1986 creates offences of stirring up racial and religious hatred, but does not cover sex. Scotland has separate offences under the Hate Crime and Public Order (Scotland) Act 2021. The Terrorism Act 2000 and the Terrorism Act 2006 cover support for proscribed organisations, encouragement of terrorism and the dissemination of terrorist publications.

The Sexual Offences Act 2003 (England and Wales) covers offences against children, including causing or inciting sexual activity, arranging a child sex offence, meeting a child following grooming and sexual communication with a child, as well as sexual activity without consent and cyberflashing. Section 66B, inserted by the OSA, criminalises sharing or threatening to share an intimate image without consent,

including synthetic NCII. The Data (Use and Access) Act 2025 added an offence around the creation or requesting a 'purported intimate image' of an adult and has been in force since 6 February 2026. The Protection of Children Act 1978 and the Criminal Justice Act 1988 criminalise indecent images of anyone under 18, which would cover images used in the sexual extortion of boys. Scotland and Northern Ireland have separate sexual offences and intimate image legislation.

Section 2 of the Suicide Act 1961 makes it an offence to encourage or assist another person's suicide or attempted suicide. The Coroners and Justice Act 2009 confirmed that this applies online, even if no suicide attempt occurs. This amended the equivalent provision in the Criminal Justice Act (Northern Ireland) 1966. Scotland has no specific offence of encouraging or assisting suicide.

The Crime and Policing Act 2026 received Royal Assent on 29 April 2026 and is the most relevant recent addition to criminal law.[1] Since 29 June 2026, offences regarding the supply of tools to generate synthetic NCII apply, alongside a 48-hour duty on digital services to remove NCII. However, the Act is rolled out in commencing stages. On 6 November 2026, offences for possessing and publishing pornography depicting strangulation, suffocation, sexual activity between relatives or of sexual activity where adults are 'roleplaying' as children came into force. Not yet commenced are offences on AI child sexual abuse image-generators, including liability for moderators of sites hosting such material, and an offence of providing AI chatbots that generate illegal content, and a broader offence of encouraging or assisting serious self-harm. However, both encouraging or assisting serious self-harm, as well as strangulation, are covered as priority offences under the OSA, meaning regulated services prevent and remove such content.

Where online abuse happens within intimate or family relationships, the Domestic Abuse Act 2021 and its statutory guidance (2022) apply, including technology-facilitated abuse, such as monitoring, threats, isolation and financial control. Controlling or coercive behaviour is an offence under the Serious Crime Act 2015 (England and Wales), which the Domestic Abuse Act 2021 extended to ex-partners. Scotland has the Domestic Abuse (Scotland) Act 2018 and Northern Ireland the Domestic Abuse and Civil Proceedings Act (Northern Ireland) 2021.

Online safety, platform and data frameworks

The OSA is the UK's core online safety regime, overseen by Ofcom. The OSA is the only UK online safety framework that covers prevention at stages 2-5 (design prevention, exposure mitigation, intervention and removal, and redress and recovery). Ofcom's statutory media literacy duty adds a general, non-harm-specific lever at stage 1 (societal prevention). The OSA imposes duties on user-to-user services, search services ('Part 3 services') and services hosting online pornography ('publishers of pornography') ('Part 5 services'). The OSA currently only applies to AI chatbots and companion services where they meet the definition of user-to-user service or are integrated into one.

For Part 3 services, these duties are to assess and mitigate risks, protect users from illegal content, and to protect children from harmful content, including through highly effective age assurance. Part 5 services are required to implement and record highly effective age assurance. Regulated services must assess the risks of users encountering illegal content and take proportionate measures, including the

[1] Most offences apply to England and Wales only.

takedown of content, where applicable. This includes content amounting to a relevant criminal offence (as outlined above), including priority offences such as terrorism, child sexual abuse material, intimate image abuse, fraud, harassment and encouragement of suicide or serious self-harm.

The OSA sets out user empowerment duties whereby 'Category 1 services' – the largest user-to-user platforms – must provide adult users with tools to reduce their likelihood of encountering certain legal but harmful content. Ofcom's Illegal Content Codes of Practice recommend hash matching to detect known non-consensual intimate images, including synthetic NCII, on high-risk and large services. Ofcom continues to update its harm categories, and in October 2026, it recommended adding body stigma and depression content to priority content that is harmful to children. The Secretary of State has the powers to approve this recommendation.

Ofcom's guidance A Safer Life Online for Women and Girls (November 2025) is produced under a statutory requirement in the OSA and is voluntary for services to implement. It covers recommendations on prevention, removal and redress. While it is framed around women and girls, it applies to men and boys as potential victims and as children exposed to harmful content. The OSA contains no comparable requirement explicitly for men and boys.

The UK's data protection laws covered by the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA) and Data (Use and Access) Act 2025 (DUAA) offer another legal basis against any of the harms that involve unlawful data processing. Additionally, the Information Commission's Office's (ICO) age-appropriate design code sets 15 standards of age-appropriate design based on a risk-based framework, specifically for services likely to be accessed by children. Services have had to comply with the code since 2 September 2021. The ICO also works with Ofcom on age assurance.

Following the UK Government's announcement on 15 June 2026 on restrictions on social media use by under 16-year-olds, it is expected that these will be implemented by Spring 2027. The relevant regulation is expected shortly after the publication of this report, by the end of 2026.

Drugs, medicines and health products frameworks

The Misuse of Drugs Act 1971 and Misuse of Drugs Regulations 2001 provide the core UK-wide controls on controlled drugs. As anabolic steroids are considered Class C drugs, possession for personal use is not itself an offence, but supply is. Content offering controlled drugs for sale may amount to illegal content under the OSA.

The Human Medicines Regulations 2012 regulates medicinal products, including advertising restrictions relevant to unlicensed products, such as injectables that are promoted online. The Medicines and Healthcare Products Regulatory Agency (MHRA) enforces against unlicensed medicines sold online, and the General Pharmaceutical Council's online pharmacy logo identifies legitimate online pharmacies. In England the Food Supplements (England) Regulations 2003 and the Nutrition and Health Claims (England) Regulations 2007 govern food supplements and health claims.

Consumer protections against misleading and aggressive practices and pyramid schemes, including online and influencer-driven marketing are strengthened by the Digital Markets, Competition and Consumers Act 2024. This is relevant for supplement and coaching schemes. Additionally, the Advertising Standards Authority's (ASA) CAP and BCAP Codes also regulate advertising claims,

including those relating to supplements, medicines and influencer marketing. However, they are non-binding.

The From Harm to Hope 10-year drugs strategy runs until 2031. It provides the wider policy framework for reducing drug supply, demand and harm, including prevention and treatment for young people. NHS guidance on anabolic steroid misuse raises awareness of the physical and psychological risks facing boys and young men. Additionally, UK Anti-Doping runs education, testing and sanctions, which apply to athletes in sport. The Tobacco and Vapes Act 2026 received Royal Assent on 29 April 2026 and its advertising and sponsorship ban applies from 1 June 2027.

Gambling frameworks

The Gambling Act 2005 and its 2025 amendments provide the principal statutory framework, under which the Gambling Commission licenses and sanctions operators in Great Britain, including online operators. Northern Ireland has a separate licensing regime under the Betting, Gaming, Lotteries and Amusements (Northern Ireland) Order 1985 (amended in 2022).

Following the 2023 white paper High Stakes: Gambling reform for the digital age, two sets of 2025 regulations put its main proposals into law. The Gambling Act 2005 (Operating Licence Conditions) (Amendment) Regulations 2025 introduced online slots stake limits of £2 per spin for 18 to 24 year-olds and £5 for those aged 25 and over. Additionally, the Gambling Levy Regulations 2025 introduced a statutory levy that funds research, prevention and treatment. The ASA CAP and BCAP Codes also restrict gambling advertising. Loot boxes remain outside gambling law.

Finance frameworks

The Financial Services and Markets Act 2000 outlines only authorised firms may communicate or approve financial promotions, including through 'finfluencers' and for cryptoassets. Additionally, unauthorised promotion is a criminal offence. The Financial Conduct Authority (FCA) enforces this online and has issued guidance on social media promotions and finfluencers. It also restricts speculative products such as contracts for difference (CFDs) and binary options. Under the FCA's Crypto Roadmap, a crypto authorisation regime is to be implemented by 25 October 2027.

Additionally, since October 2024, consumers have had a right to reimbursement for authorised push payment (APP) fraud under the Payment Systems Regulator's mandatory reimbursement regime. The Fraud Strategy 2026-2029 sets out protections against fraud for the public and aims to improve victim support. The OSA's fraudulent advertising duties are expected to apply from 2027 at the earliest.

Health and education frameworks

Health and education frameworks are almost entirely policy-led and focus on the first prevention level; societal prevention.

Men's Health: A Strategic Vision for England ('men's health strategy') (November 2025) is the first dedicated men's health strategy for England. It operationalises parts of the National Health Service (NHS) 10 Year Health Plan for England, which provide the wider delivery context for mental health and suicide prevention support. The men's health strategy covers mental health, suicide prevention and gambling harms. It sets out several interventions that are evidence-based and prevention-focused. These include up to £3.6 million over three years for neighbourhood-based suicide prevention focused

on middle-aged men, gambling awareness campaigns, and establishing an Academic Men's Health Network.

The Suicide Prevention Strategy for England 2023-2028 sets national priorities, including targeted action for higher-risk groups, alongside Creating Hope Together: Scotland's Suicide Prevention Strategy 2022-2032, the Suicide and Self-harm Prevention Strategy for Wales 2025-2035 and Protect Life 2 in Northern Ireland.

Youth Matters: Your National Youth Strategy (December 2025) provides a youth-focused framework aimed at strengthening health and wellbeing. This includes commitments to strengthen the availability of trusted adults, the workforce, friends and relationships, greater accessibility to activities, and education.

In education, the revised statutory guidance on Relationships Education, Relationships and Sex Education (RSE) and Health Education came into force in September 2026. It includes content on misogyny, online harms, deepfakes, consent and suicide prevention. Keeping children safe in education 2026 sets schools' safeguarding responsibilities and sit alongside the Working Together to Safeguard Children 2023 guidance. The Children Act 1989 and Children Act 2004 provide the wider statutory safeguarding framework in England. They apply to schools, local authorities and safeguarding partners and how they respond to online harms affecting children.

Violence abuse and social cohesion frameworks

Online harms affecting boys and men may involve perpetration, victimisation, radicalisation or exposure to harmful norms. Many of the violence, abuse and social cohesion relevant frameworks across the UK focus on men and boys as perpetrators or potential perpetrators.

The cross-government 'VAWG strategy', Freedom from violence and abuse: a safer society for women and girls treats misogyny as a driver of violence against women and girls (VAWG) and includes action on teacher training, healthy relationships education, synthetic images and nudification tools. Much of its delivery applies in England. In Northern Ireland, the second phase of the Power to Change campaign, led by the Police Service of Northern Ireland, Department of Justice and the Executive Office, encourages men and boys to challenge misogyny in online spaces.

The Department for Education's Educate Against Hate resources support schools in responding to radicalisation and extremist narratives, including misogynistic content. This aligns with the Department for Culture, Media and Sport's social connection framework (2026), which aims to address loneliness, isolation and community belonging. Additionally, the UK's Prevent duty under the Counter-Terrorism and Security Act 2015 requires specified authorities, including education settings, to have due regard to preventing people from being drawn into terrorism. The Protecting What Matters programme provides the wider social-cohesion and counter-extremism policy context, including work on online radicalisation, disinformation and community resilience. A Safe, Informed Digital Nation (2026) sets out a non-binding media literacy action plan.

Noteworthy regulatory cooperation networks

The Digital Regulation Cooperation Forum (DRCF) brings together the Competition and Markets Authority, the FCA, the ICO and Ofcom. Set up in 2020, it coordinates these regulators on overlapping

digital issues. Internationally, Ofcom is a member of the Global Online Safety Regulators Network (GOSRN), of which ISD is an observer.

Key instruments in Canada

In Canada, the key frameworks addressing men's and boys' online harms include a variation of existing, newly introduced and pending frameworks. Much of Canada's efforts so far rests on policy-led initiatives, particularly on the (1) societal prevention level and (5) redress and recovery level. The binding frameworks are centred around criminal law, sector-specific product rules and provincially regulated gambling and securities, with a proposed online safety regime pending.

Criminal law

Criminal law provides the main binding route against the outlined harms. The Criminal Code covers sexual offences, child sexual exploitation material, luring, extortion, harassment, uttering threats, fraud, trafficking and four hate propaganda offences and the non-consensual distribution of intimate images. Suicide is also covered and the Criminal Code makes it an offence to counsel or aid a person to die by suicide. There is no offence of encouraging self-harm.

The Protecting Victims Act 2026 received Royal Assent on 18 June 2026. Most of its provisions came into force on 18 July 2026. It creates offences of threatening to distribute intimate images (including synthetic images) or child sexual abuse and exploitation material. It also extends the intimate image offence to synthetic images, applies the child luring offence to sexual extortion and makes sexual extortion an aggravating factor in extortion. Additionally, it provides further strengthening around harassment and prosecuting Canadians abroad. Its new offence of coercion or control of an intimate partner is not expected to come into force until June 2028 at the latest. Several provinces provide civil remedies for intimate image abuse, and some, such as Nova Scotia also provide civil remedies for cyberbullying (Intimate Images and Cyber-protection Act).

The Mandatory Reporting Act requires all internet services to report child sexual abuse material and preserve data for 12 months. Cybertip.ca has been part of the National Strategy for the Protection of Children from Sexual Exploitation on the Internet since 2004 and is a designated reporting organisation under federal and provincial laws. It triages reports of child sexual exploitation and sexual extortion and raises public awareness. This highlights how a policy-first framework can turn into practical outcomes when backed by legislation.

The Anti-terrorism Act 2001 and the Anti-terrorism Act 2015 inserted terrorism offences into the Criminal Code and amended related legislation.

Online safety, platform and data frameworks

Following the announcements of Bill C-34 and Bill C-36 in June 2026, Canadian policymakers are taking the relevant steps to establish Canada's online safety regime alongside strengthened consumer and data protection.

Bill C-34, the Safe Social Media Act, introduced on 10 June 2026, proposes the regulation of social media platforms, AI chatbots and other online services, with a particular duty to protect children,

including through age-restrictions. It also sets obligations to mitigate seven types of harmful content outlined in the Bill. The seven types of harmful content are: 'Intimate content communicated without consent, content that sexually victimizes a child or revictimizes a survivor, content that induces a child to harm themselves, content, used to bully a child, content that foments hatred, content that incites violence, [and] terrorism or violent extremism content'. The Bill does not explicitly cover recommender systems. However, it recognises that design features, such as recommender systems, engagement-based feeds, autoplay and endless scrolling can increase exposure to harmful content. Additionally, it proposes obligations for AI chatbot services to mitigate harmful chatbot behaviour, and age-appropriate safeguards in addition to a restriction on accounts for under-16-year-olds, unless specific conditions are met. The Bill would also establish a new regulator, the Digital Safety Commission of Canada. Fraudulent content is currently out of scope of the Bill.

Bill C-36, the Protecting Privacy and Consumer Data Act (PPCDA), introduced on 15 June 2026, proposes additional privacy protections for individuals, alongside industry obligations to foster responsible innovation. Additionally, the Bill proposes the establishment of the Digital Safety and Data Protection Commission of Canada. The Bill would partly operationalise Canada's AI for All strategy, which also aims to promote AI literacy.

Drugs, medicines and health products frameworks

The Food and Drugs Act and the Food and Drug Regulations govern pharmaceuticals and other therapeutic products, including restrictions on advertising prescription drugs to the public. The Natural Health Products Regulations require a product licence before supplements can be sold, and the Medical Devices Regulations require a license before medical devices, such as dermal fillers, can be sold. These sit alongside the Cosmetic Regulations which prohibit substances such as mercury. Health Canada enforces these laws, including against unauthorised products sold online.

The Controlled Drugs and Substances Act controls drugs including anabolic steroids, whose trafficking and import are offences. However, possession is not an offence. The Cannabis Act and Tobacco and Vaping Products Act are among Canada's few binding rules at stage 2 – 4 as they ban youth-appealing and lifestyle promotion, including online.

The deceptive marketing provisions of the Competition Act apply to false or misleading claims about products' benefits. Influencer marketing guidance from the Competition Bureau and Ad Standards are voluntary, while provincial and territorial consumer protection legislation also applies.

The Canadian Anti-Doping Program covers performance-enhancing substances in organised sport only.

Gambling frameworks

Gambling is regulated provincially with exceptions as outlined in the Criminal Code. Provincial authorities handle licensing, advertising and age-verification. Single-event sports betting is legal and there is no national prevention framework around safer-gambling. Provincially regulated casinos, including online casinos, are subject to federal anti-money laundering controls under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act) (PCMLTFA). Loot boxes remain unregulated.

Finance frameworks

Financial harms are substantively regulated in Canada, however, mainly through provincial and territorial regimes, which vary. The Multilateral Instrument bans binary options for retail investors, and registration requirements and pre-registration undertakings for crypto-trading platforms, including annual investment limits. A Financial Crimes Agency, proposed under Bill C-29 on 1 May 2026, is pending. At the time of writing, the National Financial Literacy Strategy, which ended in 2026, has no successor and Bill C-34 would only reach financial harms through sexual extortion.

Health and education frameworks

Canada's health and education frameworks that address some of the outlined harms are largely policy-led. Canada's Men and Boys' Health and Well-being Strategy is expected in early 2027. Health Canada's What We Heard report (2026) identifies 'masculinity, online influences and health' as one of five key themes, which indicates that online harms are already on the federal men's health agenda.

The National Suicide Prevention Action Plan 2024–2027 sits under the Federal Framework for Suicide Prevention Act. The Act places a legal duty on the federal Government to establish, coordinate and publicly report on suicide prevention efforts, which gives the plan a statutory footing. This goes beyond conventional policy strategy, however, the plan itself remains policy-only. The 9-8-8 Suicide Crisis Helpline also supports recovery. The Canadian Eating Disorders Strategy 2019-2029 is a non-governmental framework.

Federal investment in youth mental health and substance-related harms runs through the Youth Mental Health Fund (2024), which focuses on ages 12-25, and bilateral health agreements with provinces and territories under Working Together to Improve Health Care for Canadians (2023). This operationalises the Canada Health Act.

The Canadian Drugs and Substances Strategy (2023) has a prevention and education pillar, and Health Canada's policy paper Preventing Substance-related Harms among Canadian Youth through Action within School Communities (2021) and its Blueprint for Action (2021) apply the Comprehensive School Health framework. Education is a provincial and territorial responsibility.

Violence, abuse and social cohesion frameworks

Violence, abuse and social cohesion frameworks are similarly policy-led. The women focused National Action Plan to End Gender-Based Violence (2022) names men and boys as a prevention priority, and Women and Gender Equality engages men and boys through its gender equality programmes.

Canada's Action Plan on Combatting Hate (2024), the first national strategy on hate also includes online hate. Its annex outlines the legal framework around hate, including the Canadian Human Rights Act (revised 1985), Canadian Bill of Rights (1960), the Charter of Rights and Freedoms (1982), and the Canadian Multiculturalism Act (1988) and provincial and territorial human rights legislation. Related measures include Changing Systems, Transforming Lives: Canada's Anti-Racism Strategy 2024-2028 and the Hate Crimes Task Force.

Additionally, the Canada Centre for Community Engagement and Prevention of Violence leads gender-responsive and evidence-based prevention of radicalisation. Much of the Centre's work holds roots in the National Strategy on Countering Radicalization to Violence.

Institute for Strategic Dialogue (ISD UK) is a company limited by guarantee in England (registered charity number 1141069 and company registration number 06581421) with its registered address at 3rd Floor, 45 Albemarle Street, Mayfair, London, W1S 4JL.

Key instruments in Ireland

Criminal law

Criminal law in Ireland captures harmful communications and hate, image-based abuse, sexual extortion, blackmail, sexual exploitation, cybercrime, fraud, coercive control, child sexual abuse material (CSAM) and terrorism-related content.

'Coco's law' – the Harassment, Harmful Communications and Related Offences Act 2020 – includes offences around the distribution or publication of intimate images without the subject's consent and where the distributor intends to cause harm or is reckless as to whether harm is caused. It also creates other offences, such as recording or sharing intimate images without consent, threatening to share them, and sending threatening or grossly offensive communications, intended to cause harm.

Additionally, the Criminal Justice (Hate Offences) Act 2024, and Criminal Law (Sexual Offences) Act 2017 and its 2019 amendments, cover offences relating to hate and sexual exploitation of children and grooming. Ireland's wider CSAM and exploitation framework also includes the Criminal Law (Sexual Offences and Human Trafficking) Act 2024.

The Criminal Justice (Hate Offences) Act 2024 creates offences aggravated by hatred against groups defined by protected characteristics. It does so by amending the Criminal Damage Act 1991, the Criminal Justice (Public Order) Act 1994 and the Non-Fatal Offences Against the Person Act 1997. The Prohibition of Incitement to Hatred Act 1989 remains the operative law for online hate speech but does not cover gender. A broader Bill that would have replaced the 1989 Act was stripped of proposed hate speech provisions in October 2024 amid political controversy, leaving only the hate crime elements to pass. Together with the Non-Fatal Offences Against the Person Act 1997 and Criminal Law Act 1997 Ireland partially transposed the EU Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law; the Commission found in October 2024 that elements of the framework decision remain untransposed. This is an example how EU frameworks may shape existing or new national legislation.

The Non-Fatal Offences Against the Person Act 1997 and Domestic Violence Act 2018 are relevant where online conduct forms part of stalking, harassment, threats, coercive control or domestic abuse. The EU Directive 2024/1385 on combating violence against women and domestic violence aims to establish a preventative and intersectional approach against violence against women and domestic violence. Ireland has until 14 June 2027 to transpose the Directive into national legislation. It will likely be operationalised by 'Jennie's law' - the Criminal Law (Sexual Offences, Domestic Violence and International Instruments) Bill.

Suicide is also decriminalised in Ireland, however, Section 2(2) of the Criminal Law (Suicide) Act 1993 makes it an offence to assist a person's suicide or attempted suicide. There is no standalone offence of encouraging self-harm, however, the Online Safety Media and Regulation Act 2022 (outlined below) considers content promoting or encouraging eating disorders, self-harm, or suicide.

The Criminal Justice (Theft and Fraud Offences) Act 2001 covers online scams, including deception and unlawful use of a computer, and the Criminal Justice (Offences Relating to Information Systems) Act

2017 covers unauthorised access and account takeover. The Criminal Justice (Terrorist Offences) Act 2005, amended in 2015 to add public provocation, sets out terrorist offences and Regulation (EU) 2021/784 on terrorist content online, addresses the dissemination of such content, including one-hour removal orders.

Online safety, platform, data and AI frameworks

Ireland's online safety framework combines EU regulation with national law, whereby Ireland's media regulator Coimisiún na Meán (CnaM) is the main regulatory authority (alongside the European Commission in some instances). CnaM also has a media literacy remit beyond its online safety supervision (further outlined in the education section).

On a national level, the Online Safety and Media Regulation Act 2022 and the Online Safety Code set obligations for video-sharing platforms. The Online Safety and Media Regulation Act 2022 also considers content promoting or encouraging eating disorders, self-harm, or suicide.

Additionally, the EU's Digital Services Act (DSA) requires designated 'very large online platforms and search engines' to assess and mitigate systemic risks, including risks to fundamental rights, civic discourse and minors, gender-based violence, and harms to physical and mental well-being, with considerations how recommender systems and platform design may contribute to these risks. Hosting services, including all online platforms must provide notice-and-action mechanisms and act on illegal content once notified. Beyond its risk-based approach, the DSA provides users with complaint and out-of-court dispute-resolution routes, and its transparency obligations, including data access for researchers under Article 40, should strengthen research, including around online harms to men and boys.

Under the proposed EU Kids Act, proposed in September 2026, the European Commission put forward safety-by-design obligations for services, as well as delayed access for children to social media platforms – requiring age verification.

Additionally, varying obligations would apply for other service types, such as AI chatbots. This proposal follows the European strategy for a better internet for kids (BIK+), which aims to protect children from illegal and harmful online content, empowering children to acquire relevant digital competencies, and for including children in decision-making around the digital environment. Moreover, the European Commission's guidelines on the protection of minors under Article 28 of the DSA further establish recommendations how to protect children online, and the proposed EU Digital Fairness Act would require further consumer protections, particularly for children.

However, data protection frameworks applicable in Ireland also provide levers against harms such as profiling, behavioural advertising and intrusive age assurance. They also establish the right to complain to An Coimisiún um Chosaint Sonraí, the Data Protection Commission (DPC). The frameworks include the EU's General Data Protection Regulation (GDPR), and Ireland's Data Protection Act 2018 (which strengthens the EU rules on specific issues, such as on data subject rights). Additionally, the DPC's Fundamentals for a Child-Oriented Approach to Data Processing apply if services are likely accessed by children.

The EU AI Act is the only legislative framework across this analysis that sets out broad rules on AI systems on a model level. The AI Act's rules on chatbots and transparency obligations around deepfakes are also relevant in this context.

Drugs, medicines and health products frameworks

The Misuse of Drugs Act 1977 (as amended) and the Misuse of Drugs Regulations 2017 and its associated regulations apply to supply of controlled drugs, including anabolic steroids. This also extends to social media and messaging services.

The Criminal Justice (Psychoactive Substances) Act 2010 covers the sale and supply of psychoactive substances not otherwise controlled, including when sold online. The National Drugs Strategy 2026-2029 outlines an integrated, health-focused framework to reduce harms from drug and harmful alcohol use.

An tÚdarás Rialála Táirgí Sláinte', the Health Products Regulatory Authority (HPRA) remit covers medicines, medical devices and other regulated health products, illegal or misleading medicinal claims, falsified and counterfeit products and unregulated online supply. The Medicinal Products (Control of Advertising) Regulations 2007 prohibit advertising prescription-only medicines to the public, which applies to influencer promotion of weight-loss injections. Additionally, the EU common logo for registered online pharmacies, in Ireland, overseen by the Pharmaceutical Society of Ireland, (An Rialtóir Cógaisíochta) indicates legitimate online supply. Many sports and wellness supplements are legally classed as foods, making the Food Safety Authority of Ireland (Údarás Sábháilteachta Bia na hÉireann) under the EU Nutrition Health Claims Regulation relevant.

Misleading claims about peptides, weight-loss products, erectile dysfunction products and other wellness-marketed supplements are not covered by drugs legislation. Depending on how they are classified, they fall under medicines law, food law, or consumer protection law

The Public Health (Alcohol) Act 2018 includes advertising restrictions relevant to digital and influencer marketing. Additionally, the Public Health (Tobacco and Nicotine Inhaling Products) Act 2023 bans the sale of vapes and other nicotine-inhaling products to under-18s. Meanwhile, Sport Ireland's anti-doping programme under the Sport Ireland Act 2015 is also relevant to performance-enhancing drugs if in the context of organised sport.

Gambling frameworks

The Gambling Regulation Act 2024 covers age protection, visibility of parental controls, a ban on gambling with credit, restrictions on advertising content, targeting and inducements and limits on advertising exposure. Additionally, it sets up exclusion and social impact infrastructure. Údarás Cearrbhachais na hÉireann, the Gambling Regulatory Authority of Ireland (GRAI) was established in 2025. Th GRAI recently also covered prediction markets, with restrictions unless licensed by the GRAI (since 1 July 2026). At EU level, the key principles on in-game virtual currencies provide a non-binding outline of EU consumer law for in-game currencies and paid random items.

Finance frameworks

Banc Ceannais na hÉireann's – the Central Bank of Ireland - Consumer Protection Code 2025 took effect on 24 March 2026. MiCA, the EU Markets in Crypto Assets Regulation applies to crypto-asset services

and their marketing with the Central Bank as competent authority. Additionally, the Banc Ceannais na hÉireann is a trusted flagger under the DSA, which should allow for an improved process in requesting the takedown of relevant content, for example financial scam content.

The Consumer Protection Code 2025 and the Advertising Standards Authority of Ireland (ASAI) Codes cover misleading advertising more broadly, whereby An Coimisiún um Iomaíocht agus Cosaint Tomhaltóirí, the Competition and Consumer Commission (CCPC), serves as a regulator in relation to the Consumer Protection Act 2007 and the Consumer Rights Act 2022. The ASAI has issued guidance on recognising influencer marketing, and the Consumer Credit (Amendment) Act 2022, and the EU Consumer Credit Directive are relevant to men's online borrowing. The proposed EU Digital Fairness Act would address dark patterns, addictive design and influencer marketing.

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 provides the anti-money laundering framework. The recruitment of 'money mules' on social media has been a focus of Garda and banking sector awareness campaigns.

Health and education frameworks

Ireland's health and educational responses to online harms affecting men and boys run through several overlapping systems, such as child safeguarding, school curriculum and policy, public and mental health strategy and media-literacy work (as also highlighted under the online safety section). Ireland's first National Men's Health Policy (2008-2013) was followed by Healthy Ireland – Men (HI-M) 2017-2021 and the current HSE National Men's Health Action Plan, HI-M 2024-2028, which covers men's health and suicide prevention but has no statutory basis. Sharing the Vision 2020-2030 provides a national mental health framework to strengthen mental health support across Ireland.

Young Ireland: National Policy Framework for Children and Young People 2023-2028 sets cross-government commitments for ages 0 to 24. The An Roinn Sláinte's, the Department of Health, Online Health Taskforce's report on online health and rights for Ireland's children and young people (2025) outlines evidence on boys' exposure to misogynistic content and recommends critical digital literacy education. The Online Health Taskforce was established in September 2024 and aims to develop a public-health response to harms caused by children's and young people's online activity.

BIK+ (as also outlined above), frames digital education and the empowerment of children. Ireland implements this through the Safer Internet Centre, including the Irish Internet Hotline, the Irish Society for the Prevention of Cruelty to Children (ISPCC), the National Parents Council and Webwise. The EU Digital Education Action Plan 2021-2027 and the EU's approach to mental health from 2023 further provide policy levers for strengthening digital skills and youth mental health.

The Children First Act 2015 and the Children First: National Guidance for the Protection and Welfare of Children (2017) set the foundation. These work together with the online safety regime. Organisations must prepare child-safeguarding statements and risk assessments, including considerations of online risks, such as sexual abuse and related harm. In schools, these expectations are put into practice through the Child Protection Procedures for Schools 2025, which schools must implement by December 2026. The procedures outline how concerns about online activity can be reported, supported and referred, making schools an institutional route for boys affected by harms

such as grooming, peer-to-peer abuse, coercive image-sharing, cyberbullying or extremist recruitment.

Within the curriculum, Social, Personal and Health Education (SPHE) and Relationships and Sexuality Education (RSE) educators have the opportunity to address some of the issues linked to boys' online experiences. The An Roinn Oideachais agus Óige's - the Department of Education and Youth - Junior Cycle SPHE specification and resources for post-primary schools cover consent, pornography, respectful relationships, image-sharing, coercion and extortion, body image, gender and gender identity, and help-seeking. An Roinn Oideachais agus Óige's Digital Strategy for Schools to 2027 further embeds online safety and ethical digital use across teaching and learning. Further guidance also requires schools to restrict phone use during the school day.

Additionally, the Department's Connecting for Life 2026-2035 strategy aims to reduce suicide and self-harm. The strategy focuses on five domains: prevention and stigma reduction, restricting means and methods, responses to people in distress, postvention and evidence, surveillance systems and supporting structures.

Violence, abuse and social cohesion frameworks

The main framework focusing on violence, abuse and social cohesion is Zero Tolerance - the Third National Strategy on Domestic, Sexual and Gender-Based Violence 2022-2026. It recognises technology-facilitated abuse, with some commitments focusing on men and boys as victims and in relation to prevention and perpetration. Additionally, An Ghníomhaireacht um Fhoréigean Baile, Gnéasach agus Inscnebhunaithe – the Domestic, Sexual and Gender-Based Violence Agency - (Cuan), sits under the Department of Justice, Home Affairs and Migration. While the National Strategy for Women and Girls 2025-2030 focuses on harassment and gender-based bullying towards women and girls, it also considers boys' attitudes and behaviour online.

Additionally, the No Excuses campaign addresses sexual harassment and violence and aims to challenge bystander attitudes, with young men as a key audience. CnaM's media literacy remit and the National Counter Disinformation Strategy both treat media literacy and critical thinking as core resilience measures.

In relation to social cohesion, the National Action Plan Against Racism 2023-2027 aims to tackle online racism and hate, while the National LGBTIQ+ Inclusion Strategy II 2024-2028 covers online abuse against LGBTIQ+ men and boys, though hate offences as outlined under the criminal law section, may also apply. The National Counter Disinformation Strategy is a related, adjacent measure: while its focus is disinformation rather than hate speech specifically, it aims to build societal resilience and trust and to counter the organised manipulation of online discourse.

International Digital Policy Comparisons

Australia

Australia is widely seen as the first country to establish a dedicated online safety regulator and online safety statute under the child-focused Enhancing Online Safety Act 2015. The Online Safety Act 2021

(AUS OSA) replaced it and establishes the primary online safety framework in Australia, tackling online harms. The eSafety Commissioner (eSafety) is tasked to implement and enforce the regime. eSafety have worked closely with industry to establish codes of practice that aim to protect Australians from unlawful content categorised as 'Class 1A' and 'Class 1B'.

Class 1A content constitutes content that 'is seriously harmful, including child sexual abuse material, pro-terror material, and extreme crime and violence'. Class 1B content is crime and violence content, as well as drug-related content.

Age-restricted content is categorised as 'Class 2' and includes online pornography (the exact classification depends on the type of pornography depicted) and other content considered as 'high-impact', including nudity, violence and drug use, as well as 'themes' such as suicide, death, serious illness, racism and family breakdown.

These classifications apply to social media services, 'relevant electronic services' such as instant messaging services, dating services or online multi-player gaming services, 'designated internet services' such as file storage services, generative AI services and other website and apps. They also apply to search engines, app stores, hosting services, internet service providers, and equipment services (relevant soft and hardware to access the classified content). Depending on the type of service, risk assessment requirements may apply. The commencement dates for these obligations began on 16 December 2023, with the latest commencement on 9 March 2026.

eSafety's Basic Online Safety Expectations (BOSE) provide a benchmark of the requirements for regulated service providers to mitigate online harms. These sit alongside safety-by-design principles. Additionally, BOSE Guidance was updated in December 2025 to align them with the new obligations for age-restricted services, as introduced by the Online Safety Amendment (Social Media Minimum Age) Act 2024 (SMMA). This framework made Australia the first country to introduce social media restrictions for children under 16 years old and requires designated services – so far these are nine social media and user-streaming services – to implement age assurance and prevent under 16-year-olds to create accounts.

Since the December 2025 deadline to implement these restrictions, preliminary evidence has shown mixed results on the effectiveness of the restrictions. For example, a research study from June 2026 found that three months after the SMMA came into force, more than 85 percent of survey participants under 16 years old were still able to use designated services.

On 15 October 2026, the Online Safety Amendment (Digital Duty of Care) Bill 2026 was introduced. It aims to impose a statutory duty of care on online services to provide a 'safe online environment' and protect users from serious harmful material and conduct, especially children. Such serious harm includes violent extremist material, sadistic online exploitation, and 'fake nude material'. For children specifically, services would be required to protect children from exposure to pornography, content that glorifies 'crime [or] encourages dangerous stunts or seriously harmful practices' in addition to content encouraging eating disorders, abuse, harassment or bullying and material promoting hostility toward women or gender equality. The duty would apply to services such as games, social media platforms and AI chatbots. This would be complemented by strengthened takedown notices and related powers, particularly around fake nude material. As part of the continued adaptation of Australia's online safety

regime, the Bill would repeal the existing industry codes, standards and BOSE framework, which would be superseded by the new Duty following a 12-month transition period after Royal Assent.

New Zealand

New Zealand does not yet have an online safety regime comparable to the UK, EU or Australia. Instead, it addresses harmful and illegal online content by classifying it as 'objectionable' in New Zealand. Objectionable content includes 'torture, sexual violence, sexual activity involving children or young people, the promotion of crime acts of terrorism, degrading and dehumanising conduct, extreme violence including executions, mass shootings, suicide or extreme cruelty towards animals'.

Objectionable content is 'illegal to view, share or create', and is rooted in the Films, Videos and Publications Classification Act 1993. Te Mana Whakaatu, the Classification Office, oversees the classification of content. It also engages in prevention work to support communities to make informed choices around online content. Enforcement lies with the New Zealand Police, the New Zealand Customs Service and the Department of Internal Affairs.

In addition, the Government's Online Safety (Minimum Age and Child Safety Risk Assessment) Bill, introduced in August 2026, would establish a standing regulator and a risk assessment regime for covered online platforms, including social-media-style services and social AI companions, based on design features, business models, algorithms, governance and use of technology, as well as risks from illegal and harmful content and conduct, AI-generated or manipulated content and advertising. It would also impose a minimum age of 16 for holding an account on an age-restricted platform. However, the Bill had not had its first reading before Parliament dissolved on 1 October 2026 prior to New Zealand's general election and would therefore need to be reintroduced in the next Parliament.

Institute for Strategic Dialogue (ISD UK) is a company limited by guarantee in England (registered charity number 1141069 and company registration number 06581421) with its registered address at 3rd Floor, 45 Albemarle Street, Mayfair, London, W1S 4JL.