EUROPEAN
COMMISSION

Strasbourg, 10.2.2026
COM(2026) 71 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Action plan against cyberbullying

"Safer online, stronger together"

1. Introduction

"*This business is not for charity. But parents live with the risks and harms of this every day: cyberbullying. Encouragement of self-harm. Online predators. Addictive algorithms. It is up to us to protect our next generation.*"

President von der Leyen, speech at the high-profile event 'Protecting Children in the Digital Age' 2025

The digital transformation has radically changed society. It offers vast opportunities for children and young people to develop their skills and creativity. Nowadays, 97% of young people in the EU use the internet daily, and for youth aged between 15 and 24, the top source of information is social media platforms (65%). Together with AI tools, videogames, messaging apps and online communities, they connect and engage.

But these platforms also come with risks: exposure to online predators, encouragement of self-harm, addictive algorithms, dangerous online challenges, and cyberbullying.

Fundamental rights, including children's rights, are essential to the EU's values and must be upheld both online and offline. Children and young people have the right to safely seek information, learn, be connected, and become engaged members of society. The freedoms and possibilities of the digital world must therefore be matched by our resolve to protect and empower children and young people. The promise of the digital era must not be undermined by behaviour that humiliates, excludes or harms.

Cyberbullying erodes trust and damages self-esteem. It excludes people and limits their potential. It undermines our shared ambition of a vibrant, inclusive, digital Europe for our children and youth.

Social media is a primary channel through which children and adolescents are exposed to cyberbullying, and there is mounting evidence that their exposure to inappropriate online content is having lasting, damaging effects. The EU already has a comprehensive legal and policy framework to protect and empower children online, the Digital Services Act (DSA) being the main existing tool in this regard.

As announced in the 2025 State of the Union, President von der Leyen is seeking expert advice on social media age restrictions in Europe in light of online risks, with recommendations expected by the summer 2026. A number of Member States are considering taking steps to introduce enforceable minimum ages for access to social media and requirements for parental consent and control. This includes aligning age thresholds for social media access to the digital consent age, mandating privacy-by-default for minors and setting up solutions for anonymous age verification.

A coordinated European approach to age thresholds would ensure all European children receive equal protection and would prevent legal fragmentation in the single digital market. The expert panel will pave the way to a coordinated, potentially legislative European approach to age thresholds and an evidence-based awareness-raising campaign, empowering parents to take effective control of their chidren's access to online content.

The Youth Advisory Board has also shared with the Commission President the perspectives of young people on this issue. The Commission is piloting with Member States an age-verification solution that is user-friendly, protects privacy, and is setting a ‘reference standard' in age-verification online. The European Parliament has called for a harmonised EU digital minimum age of 16 for access to social media, video-sharing platforms and AI companions, while allowing 13- to 16-year-olds access with parental consent.

The Commission will also launch an EU-wide inquiry to start an evidence-based debate on the impact of social media and excessive screentime on wellbeing and mental health of young people.

When children are online, cyberbullying remains a significant threat that requires a coordinated response at EU and national levels. The responsibility of online platforms to ensure safety by design comes first. Tackling cyberbullying requires collaboration at all levels of governance, including regulatory and law enforcement authorities, as well as a whole-of-society approach, involving parents, professionals, educators, civil society and young people themselves.

As announced in the Commission’s Political Guidelines 2024-2029, this Communication sets out a targeted action plan to firmly combat the growing trend of abusive behaviour online. It focuses primarily on children and young people, considering also the increased vulnerability of certain groups. However, many of the actions proposed will help address cyberbullying across the wider population.

The Commission will use all tools at its disposal to complement the DSA, ensuring that digital platforms take their full responsibility for detecting and fighting cyberbullying. It will support all Member States in adopting the best practices available in the EU, to maximise the effectiveness of their combat against cyberbullying. And it will step up the efforts to reach out to all parts of society with information and raise awareness of what cyberbullying looks like, how it can be prevented, and how victims can be supported.

With this action plan, the Commission invites Member States, regional and local authorities, online platforms, civil society, educational institutions, families, children and young people themselves to commit to a shared endeavour: to ensure that the digital space is safe, respectful, inclusive and supportive. The Commission proposes that our Union stands together for the mental well-being and dignity of all children and young people.

2. Cyberbullying: the issue

Cyberbullying affects children everywhere: 18.3% of children in the world have experienced cyberbullying through instant messaging, social media posts, emails, or text messages. Cyberbullying does not just occur via text but also through audiovisual content such as pictures or videos shared online.

In Europe, around 1 in 6 children aged 11 to 15 report that they have been victims of cyberbullying and about 1 in 8 admit to cyberbullying others. Between 2018 and 2022, the number of adolescents being cyberbullied rose by a quarter for boys and almost a quarter for girls. Over the past five years, cyberbullying has consistently been the main reason for contacting the Safer Internet Centres (SICs) helplines.

The 6,343 respondents aged 12-17 consulted for this action plan reported widespread exposure to cyberbullying: 1 in 4 children and teenagers aged 12-17 have experienced cyberbullying personally, and more than 1 in 3 have witnessed it.

2.1 What is cyberbullying?

Digital technologies have expanded opportunities for connection but also intensified online risks, such as social exclusion, hate offences, harassment, humiliation and abuse that can transcend physical boundaries and persist around the clock.

For the purpose of this action plan, the Commission intends to promote **a common understanding of cyberbullying**:

Cyberbullying refers to **behaviour carried out through digital technologies, with the primary intention or effect of repeatedly or continuously humiliating, socially excluding, abusing, harassing or harming in particular children or young people**.

Repetition is seen as a key feature of bullying and cyberbullying. It relates to the continuing effects on the victim, who may also fear that a one-time event could be repeatedly shared online, extending the trauma and leading to re-victimisation without further direct involvement from the perpetrator.

Power imbalance is central to bullying, but it may manifest differently online. In traditional bullying, power imbalance often derives from physical strength, social status or group norms. In cyberbullying, it also stems from unequal levels of digital influence, digital skills, access to technology, or control over content.

Cyberbullying is increasingly harder to address as it can occur on private devices anytime, anywhere, without the perpetrator's physical presence. Furthermore, it also occurs on non-publicly available channels.

The most common forms of cyberbullying include mean or hurtful comments, spreading rumours online, or sharing embarrassing or humiliating posts.

The anonymity, the wide reach in audience, and the ability to send private messages to individuals at any time, amplify the damage of traditional bullying. Moreover, digital environments foster moral disengagement, reduced empathy, and online disinhibition, lowering the barriers for online aggression.

Harmful content can remain online indefinitely. It can be continuously accessed and reshared, or made viral, which amplifies harm, causes re-victimisation, and hinders recovery. These factors must be considered in providing effective support. This expands the potential audience, enabling a continuum of aggression between physical and online spaces or vice-versa.

The ongoing rapid digital development means that the environments and tools used to inflict harm are continuously changing. To ensure flexibility, the latest technologies should be used to detect and address it.

In particular, whilst artificial intelligence (AI) may help in detecting cyberbullying, the growing adoption of AI, specifically generative AI (GenAI), and its integration into online apps and services, increases cyberbullying risks and tools or even creates new ones. For example, deepfakes have been on the rise and increasingly lead to sexually explicit deepfake abuse overwhelmingly targeting women and girls, including in cases of cyberbullying, and venturing from harmful behaviour into criminal offences when it comes to the creation of images that constitute child sexual abuse or gender-based cyber violence. This introduces an additional dimension of harm that not only damages reputation but, like other cyberbullying behaviours, could also lead to psychological trauma, underlining the urgency of monitoring and addressing these emerging risks at EU-level.

Cyberbullying and hate offences may overlap when cyberbullying is motivated by hatred or incites to violence and hatred and targets individuals by reference to certain protected characteristics. Council Framework Decision 2008/913/JHA requires Member States to criminalise the public incitement to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or ethnic origin. It also requires Member States to ensure that additional penalties are provided for criminal offences committed with racist or xenophobic motivation.

Cyberbullying may overlap with child sexual abuse within the meaning of Directive 93/2011 on combating the sexual abuse and sexual exploitation of children and child pornography.

The Directive 2024/1385 on combating violence against women and domestic violence requires the Member States to ensure that gender based cyber incitement to violence or hatred is punishable as a criminal offence. It also criminalises other cyber violence offences that often occur in the context of cyberbullying: the non-consensual sharing of intimate or manipulated material, cyber stalking and cyber harassment. The Directive also includes provisions to enable the prompt removal of illegal cyber violence material.

2.2 Groups at risk of cyberbullying

Cyberbullying is particularly prevalent among **school-aged children and adolescents**, especially as their online activity increases.

Girls and young women are exposed to bullying of a sexist and misogynistic nature and are disproportionately affected, for example, by the non-consensual sharing of intimate images and sexually explicit deepfakes.

Vulnerable groups are disproportionately exposed to cyberbullying, as cyberbullying may be directed at an individual for their perceived belonging to such groups.

Children from low-income households are more exposed to cyberbullying than their peers.

Children and young people with disabilities experience higher levels of online victimisation, including sexual and gender-based violence. Some even withdraw from digital spaces due to constant abuse.

Ethnic and religious minorities, migrants and refugees face elevated risks of racist or discriminatory bullying. For example, Roma people and other racial or ethnic minorities are particularly exposed to online harassment and illegal hate speech linked to systemic exclusion, and 90% of Jewish Europeans reported experiencing antisemitism online in the past year.

Among **LGBTIQ+ people,** 63% have often encountered violent online content against the LGBTIQ+ community. Furthermore, 11% reported that someone posted offensive or threatening comments about them on the internet in the past year, and two-thirds have experienced ridicule or harassment during their time at school.

The actions put forward in this action plan will contribute to addressing cyberbullying for any victim. The equality considerations outlined above will be taken into account in the implementation to enhance the impact of the actions.

2.3 The impact of cyberbullying

The consequences of cyberbullying can be severe and long lasting, both for individuals and for society at large. In the short run, cyberbullying can be a first step towards more serious crime or abuse, including sexual abuse.

Victims of cyberbullying face an increased risk of anxiety, depression, loneliness, self-harm, and suicidal behaviour, and are more prone to behavioural problems, including harmful coping behaviours. Moreover, those who experience cyberbullying may engage in cyberbullying themselves, if only in an attempt to escape their role as a victim. This requires a careful and child-friendly response.

Cyberbullying can also harm academic performance, student well-being and the school environment. This can have long-term consequences for educational and career trajectories, as well as students' overall well-being and satisfaction with life.

Impact on children and young people can thus have far-reaching consequences for society, exacerbating existing inequalities.

3. The way forward

There is a need for a more robust, consistent and coordinated EU response to cyberbullying that strengthens prevention and digital literacy efforts, as well as improves and simplifies reporting and victim support across the Union. Our vision is of a Europe where every child and young person can grow up free from cyberbullying, protected in their dignity, and empowered to thrive in a digital world that respects European values. To that effect, this action plan is grounded on three inter-linked pillars: A coordinated EU approach, prevention and awareness, and reporting and support.

This call for action is supported by public opinion: more than 9 in 10 Europeans state that it is urgent for public authorities to take action to protect children from cyberbullying. The public consultation supporting this plan showed strong support for digital literacy and empathy-building programmes in schools and teacher training, and for improved reporting tools and support services for victims.

3.1 Pillar I: A coordinated EU approach to protection

The Commission will make full use of the existing policy and legal instruments, and identify opportunities to combat cyberbullying as part of future initiatives. Moreover, **Member States are invited to translate common objectives into effective national measures and build an integrated and well-functioning ecosystem to tackle cyberbullying.**

The DSA remains central to enforcement efforts, requiring providers of online platforms accessible to minors to ensure a high level of privacy, safety and security of minors on their service.

Furthermore, the DSA guidelines on online protection of minors set out measures that online platform providers should put in place to comply with that obligation, including appropriate measures to reduce the risk of minors being exposed to harmful content, such as designing recommender systems in the best interests of the minors, or to harmful behaviour, including contact-related risks from interactions with peers. To protect cyberbullying victims, they further include user control and empowerment measures, child-friendly reporting mechanisms and complaint tools as well as content moderation in the official languages of the Member State where the service is provided. The DSA also requires providers of online platforms to put in place easy-to-access and user-friendly mechanisms allowing all users, including minors, to report illegal content, e.g. certain forms of illegal hate speech; or child sexual abuse material. Depending on national legislation, forms of cyberbullying may also be illegal. Providers must take prompt decisions upon the receipt of such notices.

This action plan will inform the upcoming review and update of the DSA guidelines on online protection of minors. In particular, the guidelines could help providers of online platforms design more efficient reporting tools, e.g. with regard to their visibility, technical accessibility, and linguistic regime, and use effective technologies for preventing exposure to cyberbullying. The guidelines could also help providers in designing appropriate measures to react to notifications by minors, e.g. by supporting users in storing information that can serve as evidence.

The DSA also provides for the possibility to have “trusted flaggers”, expert entities whose notices must be prioritised. These provisions may be used to address cyberbullying, with trusted flaggers contributing to tackling the dissemination of illegal cyberbullying content. The Commission will issue guidelines on trusted flaggers that will help to clarify their role in tackling illegal content, including illegal cyberbullying. Those guidelines will also help clarify providers of online platforms’ obligations as regards notices submitted by trusted flaggers.

Cyberbullying can also take place via audiovisual content online. The Audiovisual Media Services Directive (AVMSD) sets out general requirements to protect minors, in particular online, from harmful content that could impair their physical, mental or moral development. This includes content constituting cyberbullying. The AVMSD requires video-sharing platforms to take appropriate measures to avoid that minors access harmful content through the inclusion of media content standards in terms and conditions or parental control and content rating systems. Furthermore, the Member States have an obligation to protect human dignity when implementing the AVMSD. The ongoing evaluation and review of the Directive will assess how effectively video-sharing platforms have applied these rules, and whether more needs to be done to protect minors from harmful content online, including in relation to cyberbullying, and in alignment with the DSA.

The Artificial Intelligence Act prohibits AI systems that manipulate or deceive persons by exploiting vulnerabilities linked to their age, in order to distort their behaviour causing significant harm. These prohibitions can prevent cyberbullying. The Commission adopted guidelines on the prohibited AI practices to facilitate consistent and effective implementation across the Union. The AI Act also establishes transparency requirements, including the obligation to inform users when they are interacting with AI and to clearly label AI-generated or manipulated content, such as deepfakes, to prevent deception.

Furthermore, these policies must be complemented by data collection on cyberbullying, which is currently inconsistent, hindering a comprehensive understanding of trends across Member States. In response to the call emerging from the public consultation, the Commission will facilitate consistent and comparable data collection on cyberbullying across the EU, for instance providing guidance such as a common data collection framework and indicators, and the launching of EU-wide surveys via the Better Internet for Kids (BIK) platform in cooperation with other child and youth participation mechanisms. Adequate resources will be provided to enable the Safer Internet Centres (SICs) network to take on these additional tasks and ensure the long-term continuity of this work.

The Commission will:

1. expand the focus on tackling cyberbullying in the **review of the DSA guidelines on the protection of minors**, in particular with regard to measures to further prevent exposure to harmful content, and to improve the reporting systems of online platforms - scheduled in **2026**;

2. **adopt DSA guidelines on trusted flaggers** which will help clarify their role in tackling illegal content, such as illegal cyberbullying, – **by Q2 2026;**

3. assess ways to address cyberbullying on video sharing platforms in the ongoing **evaluation of the Audiovisual Media Services Directive (AVMSD) and its review – by Q3 2026;**

4. **support the effective implementation of the AI Act provisions on prohibited AI practices,** including when they are used for cyberbullying, through coordination within the AI Board and the guidance provided with the Commission guidelines on prohibited AI practices – **from Q3 2026;**

5. **facilitate the effective implementation of the AI Act transparency obligations, including through a code of practice on marking and labelling of AI-generated content**, which aims to support compliance with the AI Act transparency obligations related to marking and labelling of AI-generated content, including that used for cyberbullying – **from Q3 2026.**

The Member States are invited to:

1. establish **comprehensive national anti-bullying, including cyberbullying plans**, benefiting from the support by the EU network on children's rights in line with the Commission communication and recommendation on integrated child protection systems;

2. use the common understanding of cyberbullying put forward by this action plan to **collect consistent, comparable data on cyberbullying** facilitated by Commission support through the network of the Safer Internet Centres and the Better Internet for Kids platform, and to jointly work towards common standards in tackling cyberbullying across the EU.

3.2 Pillar II: Prevention and awareness

The best way to combat cyberbullying is to act before harmful incidents occur. Preventing cyberbullying requires healthy digital practices from an early age. It means equipping children, young people, and adults with the skills and confidence to speak about and to recognise online risks. It is also important to address the underlying attitudes that can lead to harmful behaviour online.

To be effective, prevention efforts must involve bystanders, peers, perpetrators, parents, carers, educators, and the wider school community, with the support of all relevant actors, in particular civil society organisations. This was supported by 62% of the public consultation respondents, who stressed the need to support professional training for educators, law enforcement, and social workers.

Prevention and awareness initiatives should also take place both in informal and non-formal learning environments, such as youth centres, sports clubs, and community settings, where children and young people spend much of their time. Such initiatives should also integrate the prevention of and fight against any forms of discrimination, in synergy with the EU equality strategies.

Digital education and digital literacy are increasingly needed to navigate the online world safely and responsibly. Informing children and young people about the importance of being respectful and responsible in digital environments can reduce instances of intentional or unintentional harm. This is also a preventive measure envisaged under the Directive on combating violence against women and domestic violence.

Children and young people, including those with special needs, disabilities or in vulnerable situations, should be actively involved in the design and delivery of awareness-raising activities which are empowering, inclusive and accessible, and break the silence around cyberbullying.

The Commission will make a range of prevention and awareness tools available at EU level, developed in partnership with children and young people, parents, educators, mental health professionals, and Member States, as well as civil society organisations.

As part of the digital education action plan (2021-2027), the European Commission will update its guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training. In addition, as announced in the communication on the European Democracy Shield, the updates will reflect developments in AI and social media and include teaching material and activities on cyberbullying and paying attention to inclusion and diversity. The European Commission will also develop an EU citizenship competence framework along with guidelines to strengthen citizenship education in schools.

Moreover, digital literacy, prevention of cyberbullying, and digital well-being will be areas of focus in the 2030 roadmap on the future of digital education and skills. The 2030 roadmap will aim to ensure that young people are supported in building healthy online habits and informed about the responsible use of digital devices both inside and outside of the classroom.

This work on digital literacy builds on initiatives that the Commission is implementing through the Erasmus+ programme and the European Solidarity Corps, the European School Education Platform (ESEP) and eTwinning. In the context of ESEP, the Commission will enable better and permanent visibility to all materials useful for schools on bullying, including cyberbullying. From the 2026 Erasmus+ call, well-being at school will be strengthened to better support, monitor, and encourage projects addressing bullying and cyberbullying.

The EU network for the prevention of child sexual abuse will help promote children’s education and awareness in relation to child sexual abuse, including considering initiatives to help prevent cases of cyberbullying from escalating to criminal behaviour (e.g. dissemination of child sexual abuse material). In addition, cyberbullying prevention will also be considered in the upcoming EU action plan on the protection of children against crime. The action plan will seek to provide a coherent and comprehensive response to the various risks faced by children in relation to crime, both online and offline.

The Better Internet for Kids (BIK) platform and its network of SICs provide support tools for children, parents, educators, and professionals at EU (BIK) and national (SICs) level. These resources will be further expanded to strengthen capacities, reach more stakeholders, and respond to new cyberbullying challenges.

As schools play a key role in preventing cyberbullying, awareness-raising activities will be carried out with the support of the SICs and the BIK platform starting with the annual “back-to-school" campaign at the start of each new school year, to equip teachers and children with training materials, tools, and information on how to prevent and report cyberbullying.

Resources and training on cyberbullying for non-formal and informal education will be boosted through European platforms. These include the European Youth Portal, the one-stop shop to raise awareness and promote opportunities for young people, and the European School Education Platform, the meeting point for the school education community and the Learning Corner, providing teachers and education professionals with resources and toolkits on EU initiatives.

Events like the European Youth Week and the European Week of Sport facilitate engagement on a variety of topics, including the fight against cyberbullying. The Open Method of Coordination group on the fight against hate speech in sport, established in the context of the EU work plan for sport, is working on recommendations for Member States and stakeholders for the sport environment at large, including online. Its report is expected by the end of 2026 and will include recommendations to counter cyberbullying.

The Commission will:

6. **address cyberbullying** in the **update of the guidelines for teachers and educators on tackling disinformation and promoting digital literacy** through education and training – **by Q2 2026;**

7. **strengthen citizenship education in schools** through an EU citizenship competence framework and guidelines – **in 2027;**

8. **strengthen** digital competence, **cyberbullying prevention** and digital well-being through **the 2030 roadmap on the future of digital education and skills** – **by Q3 2026;**

9. contribute to **cyberbullying prevention** in the forthcoming **EU action plan on the protection of children against crime – by Q3 2026**

10. **expand cyberbullying resources and training** for schools and for non-formal and informal education, accessible for persons with disabilities, via the BIK platform, the SICs, the European Youth Portal, and the European School education Platform – **from Q2 2026;**

11. support the Open Method of Coordination group on the fight against hate speech in sport in its work on **recommendations for countering cyberbullying in the sport environment** – report due by **Q4 2026.**

Member States are invited to:

3. strengthen prevention and early identification of cyberbullying with **clear guidelines and training for stakeholders** such as educators, carers, professionals working with children in different domains (e.g. health, sport, justice, law enforcement);

4. **strengthen child participation** in policy design and implementation of measures for child well-being;

3.3 Pillar III: Reporting and comprehensive support

Victims of cyberbullying must have clear, trusted, and accessible channels to report abuse and obtain help, including for cyberbullying through private messaging. To be effective, support efforts must extend beyond helping only victims of cyberbullying to also reach bystanders, perpetrators, parents, carers, educators, and the wider school community.

The Commission will promote coherent, EU-wide reporting possibilities and victim support. Reporting should swiftly lead to multidisciplinary support, both online and offline. It should involve all relevant authorities at all levels, private actors, civil society organisations, as well as parents, carers, children and young people themselves.

Building on insights gathered through several targeted consultations, **the Commission will support the roll out of an online safety app across all Member States**, based on successful existing national practice models, such as the French *3018 app*. The app will provide a secure, user-friendly, and confidential tool that enables children and young people to:

i. **easily report cyberbullying** to a **helpline**,

ii. **safely store and transmit evidence** in line with national legal frameworks, and

iii. receive **tailored assistance through coordinated referrals** to e.g. law enforcement, education, and child protection services.

The Commission will support the Member States, where needed and relevant, to:

i. **adapt the app to the national context and needs** (e.g. translation, branding, connection to relevant national services for support and platforms for reporting), provide features such as secure reporting, evidence preservation in line with national law and guaranteed confidentiality;

ii. **ensure interoperability** with existing infrastructures and support systems, and

iii. **support the promotion** of the uptake of the app among Member States, users and online platforms.

Online platforms will remain responsible for establishing effective reporting mechanisms. This may amount to one of the measures put in place to ensure compliance with DSA obligations on protection of minors. Complementing these efforts, the app will be made available to online platforms for integration into their reporting and user-support tools, including through Application Programming Interfaces (APIs) making it resource efficient and effective to report and respond.

The success of the app depends on the availability of support and follow-up by national authorities. Member States will play an important role in ensuring that reporting via the app is backed up by coordinated offline support (e.g. legal, social, psychological and educational support) as well as in communicating the benefits of the app. The app will aim for synergies with well-established reporting mechanisms in Member States for reporting child sexual abuse material and violence against women online, as well as EU, national and international helplines, notably child helplines (116 111) and missing children hotlines (116 000).

The Commission will adopt the next EU strategy on victims' rights in 2026 to complement EU rules with non-legislative measures. The Strategy will promote structures for targeted support (e.g. medical examination, emotional and psychological) and protection services for child victims, including those of online crime. These will also address the victims of cyberbullying in the Member States where such acts are criminalised under national law.

Under the General Data Protection Regulation, the right to have personal data erased is particularly relevant where a data subject has given consent as a child and may not have been fully aware of the risks involved, including in the context of cyberbullying. The Commission will continue to support data protection authorities in developing child-focused tools to protect social media data, prevent data or account theft, and enable the exercise of their rights.

The Commission will:

12. **support the roll out across Member States of an accessible online safety app** for easy reporting of cyberbullying, adapted to national contexts, in synergies with existing reporting mechanisms, including helplines and hotlines, fostering multidisciplinary support online as well as offline – **from Q3 2026;**

13. address child victims and online victimisation, which may include cyberbullying, in the next **EU strategy on victims' rights – 2026.**

Member States are invited to:

5. analyse their national context with a view to make available a **national online safety app** with tailored support, and, building on successful existing national practice models, **customise such a model to the national setting**, including e.g. translation, branding, connection to relevant national services for support and platforms for reporting, while ensuring core features such as secure reporting, evidence preservation in line with national law and guaranteed confidentiality;

6. ensure that reporting via the national online safety app is integrated with **a holistic and well-functioning ecosystem for case management and support**, including coordinated support offline (e.g. legal, police, social, psychological and educational support services);

7. **make the national online safety app available to online platforms for integration into their reporting and user-support tools**, including through Application Programming Interfaces (APIs), making it resource efficient and effective to report and respond;

8. **promote the wide uptake and use of the national safety app by all relevant stakeholders;**

9. **promote tools developed by the data protection authorites** in their national languages for children to protect themselves from online risks, such as cyberbullying, data or account theft, attempted scams, sexual blackmail.

4. International outreach and multi-stakeholder cooperation

The EU aims to safeguard the well-being and rights of children within its borders, but also contribute significantly to fostering a safer, more inclusive digital environment worldwide. Safer Internet Day is now a global campaign that calls upon stakeholders to jointly take action to make the internet a safer and better place for all, especially for children and young people, raising awareness of key online challenges and emerging concerns and trends.

The protection and empowerment of minors online is a global priority. This is reflected in the EU international digital strategy. The EU co-funded network of hotlines in Member States to tackle the dissemination of child sexual abuse material online is part of the INHOPE network with currently 57 hotlines operating worldwide.

The Commission will continue to engage with like-minded regulators on online safety, including preventing and addressing cyberbullying, under administrative arrangements (e.g. at present with Ofcom in the UK and the eSafety Commissioner in Australia) and digital partnerships (e.g. with Canada, Singapore, India).

The EU will promote a cooperation against cyberbullying in international fora, in line with the Global Digital Compact. UN organisations have developed guidance and tools that can be used as good practices and benchmarks, including from UNICEF (website and open-source APIs), the International Telecommunications Union (guidelines on child online protection), as well as from the Special Representative of the UN Secretary General on violence against children. The EU supports UNESCO's outreach to regulators to implement the UNESCO guidelines on the governance of online platforms.

The EU funds dedicated awareness and protection support programmes for children in non-EU countries, in particular candidate and neighbouring countries, online and offline, through the NDICI-Global Europe instrument. The EU also supports alignment with EU rules under the accession process for candidate and potential candidate countries, and promotes the online safety of children and young people in neighbouring countries by exchanging knowledge and best practices through the Safer Internet Centre+ (SIC+) programme.

5. Next steps

The Commission will monitor the implementation of the action plan across all three pillars, working closely with Member States, SICs, and other stakeholders. Progress, challenges and good practices will be tracked through existing tools such as the annual BIK Policy Map, reports from the SICs and regular exchanges through expert fora, ensuring transparent and participatory monitoring.

The Commission will work with Member States to embed monitoring frameworks into national cyberbullying strategies or policies, assessing implementation, accessibility, inclusiveness, and adaptability to evolving digital contexts, with involvement of children and young people.

Findings will be shared at EU level to support mutual learning and policy alignment, informing updates to initiatives under BIK+ and the DSA.

The Commission will take stock of this action plan in 2029, including through consultations with children and young people.

6. Conclusions

> *“We want a safe online space for children, for youth, and for the next generation but we do not have it yet. We have some problems. And these are problems not just for this generation. So, we need some help from the EU to make our safe online spaces. You have to start somewhere. We have to do it now. For the future.”*

A quote from children who are members of the EU Children’s Participation platform

Children and young people reach out to us with a call for help to make online spaces safe, for them, their peers, and future generations. We must rise to the challenge across our entire Union, because protection and empowerment of our children and youth should not depend on a postcode.

Building on an already robust EU toolbox of legal and policy measures against online harms and drawing on contributions from a wide range of stakeholders, this action plan will help build a safe, inclusive and empowering digital environment for children and young people in Europe. It will complement and inspire ongoing EU initiatives on safer internet, platform responsibility, digital skills and education, child and youth empowerment, data collection, and international cooperation.

The Commission invites the European Parliament and the Council to endorse this action plan and work together on its implementation. The Commission calls on the Committee of the Regions and the European Economic and Social Committee to promote dialogue with local and regional authorities, economic and social parties and civil society.

ANNEX: Key Actions and Timeline

Pillar I: Coordinated EU approach to protection

The Commission will:	
expand the focus on tackling cyberbullying in the review of **the DSA guidelines on the protection of minors;**	2026
adopt **DSA guidelines on trusted flaggers** which will help to clarify their role in tackling illegal content, such as illegal cyberbullying;	by Q2 2026
assess ways to address cyberbullying on video sharing platforms during in the ongoing **evaluation of the Audiovisual Media Services Directive** and its review;	by Q3 2026
support the **effective implementation of the AI Act provisions on prohibited AI practices**, including when they are used for cyberbullying;	from Q3 2026
facilitate the **effective implementation of the AI Act transparency obligations related to marking and labelling of AI-generated content**, including when it concerns for cyberbullying.	from Q3 2026

The Member States are invited to:
establish **comprehensive national antibullying, including cyberbullying, plans**, notably with the support of the EU network on children's rights;
collect consistent, comparable data on cyberbullying facilitated by the network of the Safer Internet Centres and the Better Internet for Kids platform.

Pillar II: Prevention and Awareness

The Commission will:	
address cyberbullying in the **update of the guidelines for teachers and educators on tackling disinformation and promoting digital literacy;**	by Q2 2026
strengthen citizenship education in schools through an EU citizenship competence framework and guidelines	2027

strengthen digital competence, cyberbullying prevention and digital well-being through **the 2030 roadmap on the future of digital education and skills;**	by Q3 2026

contribute to cyberbullying prevention in the forthcoming **EU action plan on the protection of children against crime;**	by Q3 2026
expand **cyberbullying resources and training** for schools and for non-formal and informal education, accessible for persons with disabilities, via the BIK platform, the SICs and the European Youth Portal;	from Q2 2026
support the Open Method of Coordination group on the fight against hate speech in sport in its work on **recommendations for countering cyberbullying in the sport environment.**	by Q4 2026

The Member States are invited to:
strengthen prevention and early identification of cyberbullying with **guidelines and training for stakeholders** such as educators, carers, professionals working with children in different domains;
strengthen child participation in policy design and implementation of measures for child well-being;

Pillar III: Reporting and comprehensive support

The Commission will:	
support the roll out of **an accessible online safety app** across Member States;	from Q3 2026
address child victims and online victimisation, which may include cyberbullying, in the **EU strategy on victims' rights.**	2026

The Member States are invited to:
analyse their national context with a view to make available **a national online safety app** and, building on successful existing national practice models, customise such a model to the national setting;
ensure that reporting via the national online safety app is integrated with **a holistic and well-functioning support ecosystem;**
make the national online safety app available to online platforms for integration into their reporting and user-support tools;

promote the national online safety app among relevant stakeholders.
promote tools developed by the data protection authorites in their national languages for children to protect themselves from online risks, such as cyberbullying.