

CyberGuard

Guide for Preventing and Combating Cyberbullying

CYBERGUARD

Learning Strategies for Preventing, Intervening, and Empowering Youth Against Cyberbullying

Project Number:
2025-1-CZ01-KA210-YOU-000365051

2026

PRINCEPS
RISK INTELLIGENCE INSTITUTE

fifty-fifty

EduAge

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the Czech National Agency for International Education and Research (DZS). Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents



Introduction	**3**
PART 1 – Understanding Cyberbullying	**6**
PART 2 – PREVENTION AND DIGITAL LITERACY	**7**
PART 3 – Intervention and Response	**15**
PART 4 – Best Practices and Standardized Approach	**20**
PART 5 – Practical Tools (ALL)	**42**
Resources	**42**

Introduction

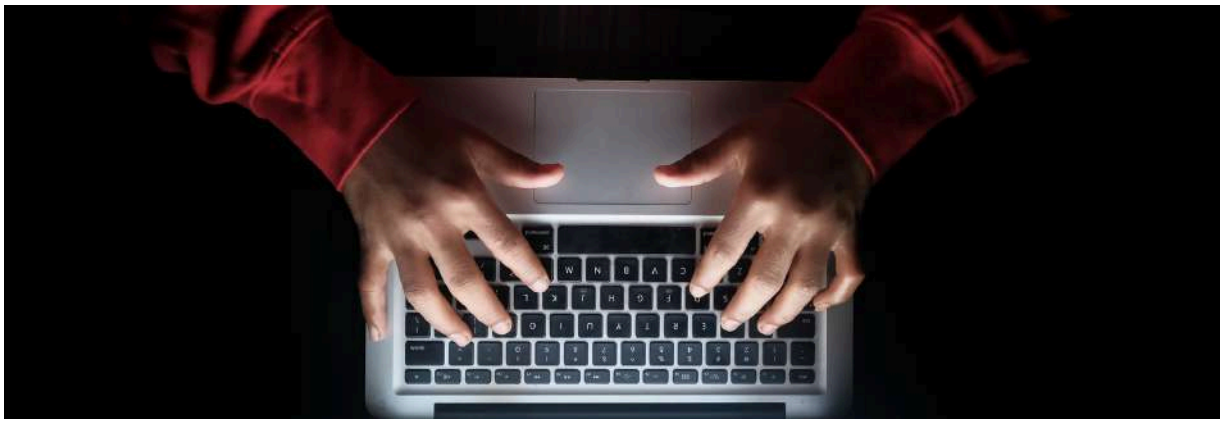
Purpose of the Guide

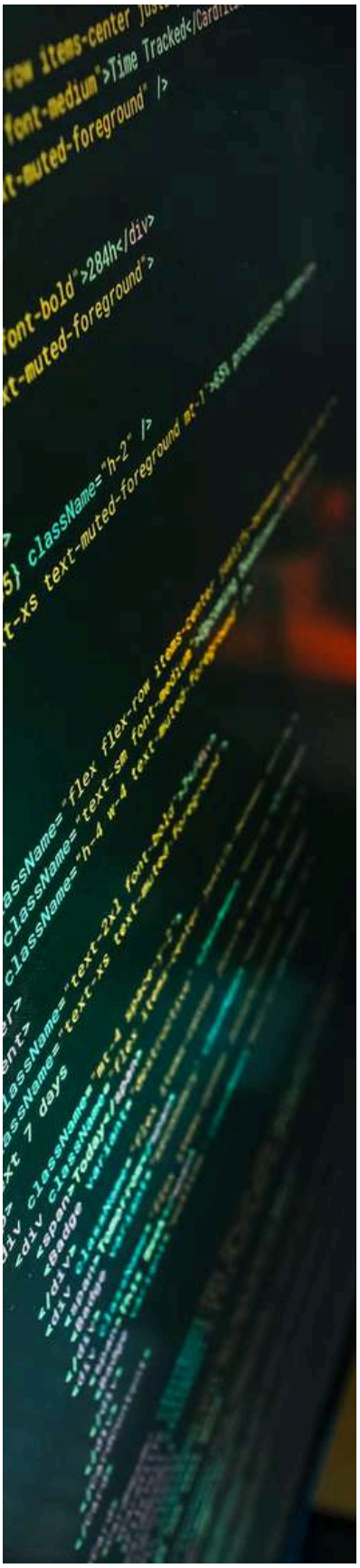
The digital environment has become an essential part of young people's daily lives, influencing communication, education, social interaction, and personal development. Alongside the many opportunities created through digital technologies, there has been a significant increase in online risks, particularly cyberbullying and other forms of harmful online behaviour. Cyberbullying constitutes a serious social and educational concern, often resulting in emotional distress, psychological harm, social isolation, and reduced participation in educational and community life.

The CyberGuard Guide for Preventing and Combating Cyberbullying has been developed as a comprehensive educational and practical resource dedicated to strengthening prevention, intervention, and support mechanisms related to cyberbullying. The guide seeks to provide professionals, institutions, and organisations with structured knowledge, practical methodologies, and effective approaches capable of addressing the complex challenges associated with digital violence and online harassment among young people.

Special emphasis is placed on strengthening digital resilience, fostering respectful online interaction, encouraging responsible digital participation, and supporting the creation of safe and inclusive digital environments. The guide combines theoretical understanding with practical tools and evidence-informed approaches, ensuring that readers are equipped with applicable strategies suitable for educational, youth work, and institutional contexts.

Developed within the framework of the Erasmus+ CyberGuard project, this publication reflects the collaborative expertise and shared commitment of partner organisations from the Czech Republic, Bulgaria, and Greece. The content has been shaped through research activities, training sessions, workshops, and direct engagement with youth workers, educators, and young people, ensuring relevance to contemporary realities and emerging digital challenges.





Target Groups

Youth Workers

Youth workers hold a fundamental role in supporting young people facing challenges related to online behaviour, digital communication, and cyberbullying incidents. Due to their close interaction with youth in non-formal educational settings, community initiatives, and youth support structures, they frequently represent a primary source of guidance, trust, and intervention.

This guide provides youth workers with practical methodologies, response frameworks, educational techniques, and prevention strategies that strengthen their professional capacity to identify cyberbullying behaviours, respond appropriately to incidents, support affected individuals, and encourage positive digital engagement among young people. Particular attention is given to strengthening confidence and preparedness in addressing complex online situations within youth work environments.

Educators and Trainers

Educators, teachers, trainers, and school staff possess significant responsibility in shaping safe, respectful, and inclusive learning environments, both offline and online. The increasing integration of digital technologies within educational settings has created a growing need for structured educational responses to cyberbullying and harmful online conduct.

The guide offers educational approaches, awareness activities, workshop models, and practical recommendations suitable for formal and non-formal educational contexts.

The content supports professionals in addressing cyberbullying through educational dialogue, digital literacy development, critical thinking, emotional awareness, and responsible online behaviour. Furthermore, the guide contributes to strengthening institutional preparedness and safeguarding practices within educational communities.

Policy-Makers and Institutional Stakeholders

Policy-makers, public authorities, institutional representatives, and decision-makers play a central role in establishing sustainable and coordinated responses to cyberbullying at local, national, and European levels.

Effective policies, institutional procedures, and long-term strategic planning remain essential elements in addressing online violence and ensuring the protection and well-being of young people.

This guide provides policy-oriented perspectives, institutional response models, legal considerations, and examples of good practice capable of supporting the development of effective prevention frameworks and safeguarding strategies. The guide also encourages cooperation between educational institutions, youth organisations, civil society actors, and public bodies in order to strengthen collective responses to cyberbullying and digital safety challenges.

How the Guide Supports the CyberGuard Project

The *CyberGuard Guide for Preventing and Combating Cyberbullying* represents one of the principal outcomes of the Erasmus+ *CyberGuard – Learning Strategies for Preventing, Intervening, and Empowering Youth Against Cyberbullying* project. The guide contributes directly to the project's broader mission of strengthening digital safety, improving preparedness among professionals working with youth, and supporting young people in navigating digital environments safely and responsibly. The publication consolidates the knowledge, expertise, methodologies, and experiences developed throughout the project's implementation. Insights gathered through training activities, local workshops, collaborative events, and transnational cooperation have informed the structure and content of the guide, ensuring alignment with the real challenges and needs identified within partner countries and local communities.

A central contribution of the guide lies in strengthening the professional capacity of youth workers, educators, and institutional stakeholders to prevent and address cyberbullying effectively. The guide further contributes to enhancing digital literacy, supporting emotional well-being, encouraging respectful online interaction, and reinforcing inclusive approaches within educational and youth work settings. In addition, the guide supports the sustainability and long-term impact of the CyberGuard project through the provision of accessible educational resources and transferable practices that remain available beyond the project's duration. Its content is intended to serve as a practical reference point for organisations, institutions, and professionals committed to creating safer, more respectful, and more inclusive digital environments for young people across Europe.



PART 1 – Understanding Cyberbullying

We live in a digital age. Children are growing up in a world, where access to the digital environment is essential and omnipresent - 98 % of young people (aged 16-29) in the EU use the internet every day. This provides them with opportunities but also makes them vulnerable to risks, with cyberbullying being one of the most prevalent ones.

According to 2025 EU research, one in three European children aged 12-17 had seen someone being cyberbullied, while every fourth child had experienced it in the role of the victim. In the last five years, it has been the main topic of the calls to helplines of EU's Safer Internet Centres. But what is exactly cyberbullying? How does it affect the victims? How can the victims and institutions react?

What is Cyberbullying

Cyberbullying is bullying with the use of digital technologies, as it can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. It can happen anytime, anywhere, and the forms vary widely: spreading sensitive or harmful content, sending threatening messages, cyberstalking, social exclusion from groups, impersonation, etc. The seeming anonymity of the bully and physical distance are major characteristics, which differentiate bullying in the digital space from offline bullying.

According to a 2022 research on American youth, hateful messages are the most common version of cyberbullying. Girls aged 13-17 are slightly more vulnerable than boys of the same age (49% vs. 43%), and children themselves describe the "people who are different" as the most vulnerable group.

Effects on young people

Cyberbullying's effects don't end with the turning off of the digital device, and they leave a lasting impact on mental health. Affected children have difficulty concentrating, are anxious before going to school, consider avoiding classes, experience feelings of shame, isolation and powerlessness, nightmares and self-destructive thoughts. The stigma of silence and the fear of asking for help, which are commonly associated with offline bullying, are also accompanied by the pressure of a virtual world without emotional filters, accessed by youth regularly on a daily basis.

Furthermore, with young people there is a strong link between experiencing bullying and addiction to the internet, which may prove to be a form of escape. However, with cyberbullying this exposes the victim further, creating a closed loop of distress, prolonged exposure and social withdrawal. In some cases, experiencing cyberbullying may lead to self-harm and suicidal ideation.

Combating Cyberbullying

If cyberbullied, children in the EU aged 12-17 would most likely tell a parent or a carer (62%), a friend (41%), or a teacher (25%). Only 14 % of them would contact a helpline or support line. With age, the likelihood of telling a friend increases, while less children would contact their parents and teachers.

There are several effective school programmes across EU member states focused on decreasing bullying and cyberbullying, such as Olweus, NoTrap!, KiVa and FUSE, but their success depends on local circumstances and quality of implementation. Notably, many programmes focus on the primary stage or early years of secondary education, achieving their main successes there, but lose effectiveness with older adolescents.

Besides issuing recommendations for member states in the field of education, passing the Digital Services Act in 2022, and formulating an Action plan against cyberbullying in 2026, the European Union has also created a network of Safe Internet Centres (SIC) as part of the Better Internet for Kids initiative. These centres, located in each member state, typically consist of an awareness centre, helpline, hotline and youth participation services.

Still, the participation of civil society and individuals is key in combating cyberbullying as a rising phenomenon. The purpose of this guide is not only to raise awareness about this problem, but also to empower individuals and groups to take action and build resilience.

PART 2 – PREVENTION AND DIGITAL LITERACY

Promoting Digital Literacy

Digital literacy isn't about knowing how to use apps. You already know how to use apps.
It's about understanding what actually happens when you're online — why messages go wrong, why you react the way you do, and how to use that understanding to stay in control of your own experience.

Know who you are online - and notice when you lose that

Your digital persona is not the same as you. Platforms pull it in a specific direction: toward what gets liked, what gets attention, what avoids conflict. Add anonymity and an invisible audience, and the gap between the real you and the online version grows wider - often without you noticing.

This matters because of what happens when someone attacks the online persona. If you've merged with it - if you can't feel the difference between the image and you - you go all-in on defending something that isn't even really you.

As part of the CyberGuard workshops, the "Observe, Don't Merge" approach was developed as a practical reflection tool to help young people distinguish between their online persona and their broader sense of identity. When something hits you online, ask yourself one question:

"Am I reacting to what was actually said - or to what this attack seems to say about my worth?"

If the answer is the second one, you've merged. Noticing that is how you step back out. You don't need to feel nothing - you just need to see the difference between the image and you. That gap is where your freedom is.

Understand how language breaks down in digital spaces
Online, tone disappears. No voice, no face, no body language. What's left is words, and words without tone get completed by whoever's reading them.

This is why the same word can mean completely different things depending on the moment. Take "Okay." or "Fine." or "Sure." or "Whatever." each reads as neutral, dismissive, cold, sarcastic, or playful depending entirely on your state when you receive it. The message hasn't changed. Your emotional lens has.

You're completing the message. The tone you hear? You're supplying it.
Knowing this means you can pause before you react and ask: am I reading what's there ,or what I'm afraid is there?

THE PAUSE–TRANSLATE–RESPOND METHOD (PTR)
Method was developed within the CyberGuard workshops as a practical tool to support young people in managing emotionally challenging online interactions and responding in a more reflective and deliberate manner. When a difficult message lands, instead of reacting immediately, work through three steps:

- PAUSE · Stop before you respond. Take a breath. Emotions peak in the first seconds, don't let your first impulse be your answer.
- TRANSLATE · Rewrite the message in neutral, factual language. Strip away the tone, the assumptions, the worst-case reading. Example: "Why are you ignoring me?" → "Someone is asking why I haven't replied. "That one step lowers the emotional charge immediately.
- RESPOND · Choose a deliberate action:• Clarify , if a direct response will actually help• Set a boundary, if the behaviour needs naming ("I need you to stop.")• Postpone, if you're too activated right now ("I'll reply when I'm ready.")• Neutral reply, if you need to respond but don't want to invite more ("Ok.")• Silence, not every message deserves a reply.
- *Rule of thumb: if responding will help you or the other person, respond. If it'll only feed the conflict, don't.*



Why online conflict hits harder than it should

When something hostile lands online, a sharp comment, a sudden exclusion, the double tick that never turns blue, your brain responds as if there's a physical threat. Not because you're oversensitive. Because digital communication creates the exact conditions for threat response.

Online messages move faster than your brain can process them. The absence of vocal tone removes the safety signals you normally use to assess a situation. Even an imagined audience raises the social stakes. Notification loops keep background stress running throughout the day. And because your identity feels more exposed online, your defensive response activates faster.

The result is what's called a limbic hijack: your body reacts before your brain has had a chance to think. You feel the tightening in your chest, the heat, the urge to respond right now, before you've understood what you're actually reacting to. This is not weakness. This is the biology of being human in a digital environment that was not designed for human nervous systems.

Once you understand this, you can start working with it instead of against it.

Your body signals it before your mind does
Before the emotional thought arrives, your body is already responding. The CyberGuard Body Signals Map helps you identify where you feel digital stress: jaw, shoulders, chest, stomach, hands. Most people find the same spots react consistently. Learning to catch these signals early, before the emotional spiral picks up speed, is one of the most practical skills you can build.

Once you feel the signal, reach for a grounding tool.

GROUNDING TOOLS - WHICH ONE TO USE AND WHEN
4–2–6 Breathing · Use this when you feel reactive and need to slow down fast.Inhale 4 counts → hold 2 → exhale 6. Repeat three times. This lowers your heart rate and gives your brain time to catch up.
Box Breathing · Use this when you feel overwhelmed or like things are spiralling. Inhale 4 → hold 4 → exhale 4 → hold 4. Repeat twice. The even rhythm calms your system fast.
5-4-3-2-1 Sensory Reset · Use this when your thoughts are looping and you can't stop replaying the message. Name 5 things you can see, 4 you can hear, 3 you can feel, 2 you can touch, 1 you can smell. This pulls you out of the thought spiral and puts you back in the room.
Jaw Release · Use this when the tension is mostly physical, tight jaw, stiff shoulders, clenched hands. Drop your jaw, let your tongue rest, take one slow breath. This tells your body it's safe to relax.
All four take under 60 seconds. They work because they interrupt the physical reaction, not just the thought.

Your digital habits shape your emotional baseline
Most online stress doesn't come from one big incident. It builds through daily pressure. The CyberGuard Online Load Map names eight specific sources that drain you:

- Notifications — constant interruptions that keep you on edge
- Messages — the pressure of unread, unanswered, or ambiguous conversations
- Social comparison — measuring yourself against curated, edited versions of other people
- Multitasking — switching between apps and conversations without resolution
- Algorithm pressure — content designed to provoke reaction rather than genuine connection
- Screen time patterns — the accumulated weight of total hours online
- Night-time scrolling — using your phone when your brain most needs to recover
- Emotional triggers — specific accounts, formats, or conversations that consistently set you off

Your Digital Hygiene Plan is your personal response to this list. Not rules someone else wrote. Boundaries you choose, based on what actually drains you.
YOUR DIGITAL HYGIENE PLAN — FIVE SECTIONS TO FILL IN

- 1. My online stressors Which of the eight categories above hit you hardest? Name your top three.
- 2. Body signals I notice Where do you feel digital stress in your body? (jaw, chest, stomach, hands, shoulders) What does the sensation feel like?
- 3. Habits that help me regulate What already works for you? (breathing, stepping away from the screen, movement, talking to someone)
- 4. Boundaries I want to try Examples: mute notifications after 20:00 · no scrolling in the first 30 minutes of the morning · turn off read receipts in one app · keep one hour of the day device-free
- 5. My one-week commitment One specific change you will make this week. Write it as a sentence: "This week I will…"

The Observer perspective changes how you communicate
Knowing this also changes how you think about what you send. You already know the receiver will complete your message through their own emotional state, not just your intention. That alone is worth holding before you write.

In the CyberGuard Rewriting activity, the Observer perspective, the view from completely outside the conflict, is consistently the one that surprises people most. From that position, most online conflicts look small, reactive, and driven by misread tone on both sides. The content is almost never the real issue. The emotional state is. When you can hold that outside view while you're still inside the conversation, the choices you make are different.

THE CYBERGUARD OATH
At the end of the training, every participant writes one sentence — a personal commitment to their digital life. Not a rule. Not a pledge. A guiding sentence that belongs to them.
To write your own, start with one of these:"I choose to…""I will no longer…""I will protect…""I will stay aware of…""I give myself permission to…"
Examples from CyberGuard participants:"I choose clarity over reaction.""I will no longer merge with digital noise." "I will protect my inner space. ""I give myself permission to pause before I respond."

One sentence. Yours. It follows you.

Awareness and Educational Activities
The best way to build digital resilience isn't to sit and listen to someone explain cyberbullying. It's to experience something that shifts how you see it.





The CyberGuard training does exactly that. It's a four-day programme for young people aged 15–25, built around one question: what would it take for you to feel truly safe online? Not protected by rules — but actually ready, because you know what's happening and you have tools that work.

The programme was developed and piloted by EduAge in Sofia, Bulgaria, in November 2025, with 15 young people and youth workers from three partner countries: Bulgaria, Czech Republic, and Greece. Every activity below was tested in that room and refined based on what actually worked. Based on the experience of the CyberGuard training, the following four-day structure is presented as a practical blueprint for the design and implementation of cyberbullying prevention programmes. Developed and piloted during the CyberGuard workshops, it provides youth workers, educators and trainers with an adaptable framework that combines digital literacy, emotional awareness, responsible online communication and practical prevention tools. Rather than serving as a fixed training model, the structure can be adapted to different target groups, learning environments and local contexts.

The Four-Day Journey
Day 1 — The Digital Self
Who am I online, and how is that different from who I am offline?

You start with the Digital Mirror exercise: mapping the version of yourself that exists in digital spaces. Not the ideal version, the actual one. What do you post, and why? What do you hide? What version of yourself performs better online? What happens when that performance is challenged?

Most people are surprised by what comes up. Platforms reward specific behaviours, consistency, relatability, provocation, and over time your online persona drifts toward what gets engagement rather than what's true. The hit of a like, the anxiety of no response — these shape what you post before you even realise it. Day 1 names all of this.

It introduces the central practice of the whole training: Observe, Don't Merge. Watch your digital self without becoming it. Notice the gap between the persona and the person. That gap is where your freedom is.

Day 2 — Words as Weapons, Words as Shields
How does language actually work online — and how can it protect you?

In the Tone Shifts Meaning activity, you take the same word — "Okay." "Fine." "Sure." "Whatever." "Do you want something?" — and read it in three tones: neutral, irritated, playful. The shift is immediate and startling. You realise that what you hear in a message is not just what's written. You're supplying the tone, and it's coming from your own emotional state.

Then comes Rewriting Harmful Comments. Each group takes a real hurtful message and rewrites it from four perspectives: the person who sent it (what emotional state, what insecurity was driving it?), the person who received it (what did it feel like?), the Observer (someone completely outside the exchange), and a healthy version (what would a grounded, clear person actually say?).

The Observer perspective is consistently the most revealing. From outside the conflict, the comment usually looks small, reactive, and about the sender's internal world rather than the target's worth. When that clicks, the emotional weight of the comment drops — not because you're pretending it doesn't hurt, but because you've seen it clearly.

Day 2 closes with PTR practice using real message cards: "Answer me now." "Lmao you seriously think this is good?" "You didn't answer." Pairs work through Pause, Translate, Respond and share one example in plenary. The difference between reacting and responding becomes something you feel, not just understand.

Day 3 — Emotional Armor and Digital Detox
What is your body trying to tell you — and how do you listen?
You start by mapping where you feel digital stress using the Body Signals Map. Jaw, chest, hands, shoulders, stomach — you mark where the activation lives. Then you learn why it happens: why your brain reads ambiguity as threat, how notification loops run background stress throughout the day, why online speed consistently outruns emotional processing.

You try each grounding tool and find the ones that actually work for you. Then you map your digital load across the eight Online Load Map categories and look honestly at which habits drain you most.

The day ends with each participant building their own Digital Hygiene Plan — five sections, personal boundaries, one concrete commitment for the week ahead.

Day 4 — From Reaction to Creation
What happens when you turn a difficult online experience into something you made?
This is the day most participants describe as unexpected. You begin with a Story Seed Card. Three questions give you your raw material:

What happened? (one or two sentences)How did it feel? (three words only)What do I wish I had said, done, or known?

Then your group transforms that seed. You choose one of four formats: a 4-panel comic strip, a rewritten conversation with an empowered ending, a 150-word micro-story, or a metaphor poster.

The comic format makes the logic of the whole activity visible. A typical example: Panel 1 — someone posts a photo, a comment arrives: "LOL ugly." Panel 2 — a grey cloud of embarrassment, the impulse to delete everything.

Panel 3 — a shift: “This comment says more about them than about me.” Panel 4 — a grounded response, a block, or deliberate silence. Four frames. The experience moves from inside the person to on paper. It becomes something they can look at instead of something they’re trapped inside.

The mechanism is the same across all four formats. When you structure an experience into a narrative, your brain stops treating it as an ongoing threat. It becomes a completed event. The emotional charge doesn’t disappear — but it shrinks to something workable.

Day 4 closes with the CyberGuard Oath. Every participant writes one guiding sentence for their digital life.

Why This Approach Works

Each CyberGuard session follows the same sequence: direct experience first, then the concept that names it, then a transferable tool. You feel tone change in real time before anyone explains why tone matters. You rewrite something before anyone tells you rewriting helps. You notice what happens in your body before you learn the term “limbic hijack.”

This sequence matters because information without experience doesn’t change behaviour. You can know intellectually that pausing before reacting is a good idea — and still not do it. But when you’ve felt the difference between reacting and responding in your own body, and you’ve practised making the translation, it becomes a real skill rather than a piece of advice.

Every tool in the CyberGuard programme — PTR, the Body Signals Map, the grounding rituals, the Digital Hygiene Plan, the 4-panel comic — is designed to be used the following day: with yourself, with friends, in a youth group, or in a one-to-one conversation with someone who needs support.

The methodology treats young people as capable of understanding and working with their own psychology. Not as recipients of warnings, but as people with the capacity to navigate difficulty when they have the right tools.
That’s the whole point.



PART 3 – Intervention and Response

Introduction to Part 3

Responding effectively to cyberbullying requires more than immediate reaction or disciplinary measures. Meaningful intervention depends upon careful identification of harmful behaviours, structured response procedures, emotional support mechanisms, and coordinated cooperation between youth workers, educators, families, institutions, and young people themselves. As digital communication continues to shape everyday social interaction, professionals working with youth increasingly encounter situations involving online harassment, exclusion, intimidation, and emotional abuse occurring across social media platforms, messaging applications, gaming environments, and other digital spaces.

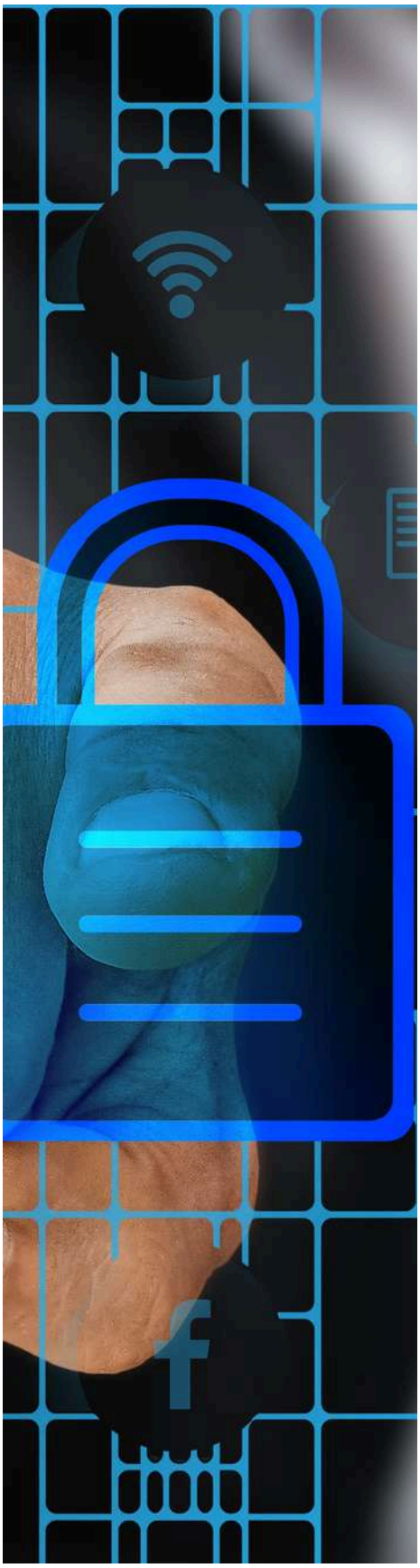
Cyberbullying often develops in ways that remain invisible to adults and institutions, while its effects may extend deeply into the emotional, psychological, social, and educational lives of young people. For this reason, effective intervention requires sensitivity, consistency, confidentiality, and a clear understanding of the responsibilities involved in safeguarding young individuals within digital environments.

This section provides a structured framework for recognising cyberbullying, responding appropriately to incidents, supporting affected individuals, and addressing harmful behaviours through educational and restorative approaches. Particular emphasis is placed on the importance of respectful communication, emotional safety, accountability, and long-term prevention within educational and youth work settings.

Identifying Cyberbullying

Understanding Cyberbullying Behaviour

The identification of cyberbullying represents one of the most important stages in the intervention process. Unlike traditional forms of bullying, cyberbullying frequently occurs in private digital spaces that may not be immediately visible to educators, youth workers, or family members. Many young people experiencing online harassment hesitate to report incidents due to fear of escalation, embarrassment, social pressure, or concerns regarding restrictions on internet access and digital devices. Consequently, harmful behaviours may continue for extended periods before intervention takes place.



Cyberbullying may involve repeated hostile communication, public humiliation, online exclusion, impersonation, dissemination of private content without consent, threatening messages, or the deliberate spread of rumours through digital platforms. Such behaviours often aim to damage an individual's emotional well-being, reputation, social relationships, or sense of security.

The impact of cyberbullying extends beyond the digital environment itself. Young people affected by online harassment may experience anxiety, emotional distress, loss of confidence, isolation, reduced academic performance, and difficulties in maintaining healthy social relationships. In severe cases, prolonged exposure to cyberbullying may contribute to depression, self-harm, or significant psychological harm.

Recognising Warning Signs

Professionals working with young people should remain attentive to behavioural, emotional, and social changes that may indicate the presence of cyberbullying. Sudden withdrawal from social activities, reluctance to participate in educational or youth programmes, visible distress after using digital devices, changes in mood, sleeping difficulties, emotional instability, or avoidance of online communication may represent important warning signs.

In many cases, victims of cyberbullying attempt to conceal their experiences, making indirect indicators particularly significant. Increased anxiety, reduced concentration, loss of motivation, social isolation, or abrupt disengagement from peer interactions may suggest underlying digital harassment or emotional distress connected to online experiences.

Attention should also be given to digital indicators such as repeated hostile messages, exclusion from online groups, circulation of humiliating images or comments, creation of false accounts, or unauthorised sharing of private information. These behaviours frequently occur simultaneously across multiple digital platforms, intensifying the emotional impact on the individual targeted.

The Importance of Early Identification

Early recognition of cyberbullying significantly improves the effectiveness of intervention and reduces the risk of long-term harm. Prompt identification allows professionals to provide emotional support, implement safeguarding measures, and prevent the escalation of abusive behaviour before it becomes deeply embedded within peer relationships or online communities.

Establishing trusting relationships with young people remains essential in encouraging disclosure and communication. Young individuals are more likely to seek support when they feel respected, understood, and confident that their concerns will be addressed sensitively and confidentially. Creating safe environments where discussions around digital experiences are normalised constitutes an important element of effective identification and prevention practices.



Step-by-Step Response Framework

Principles of Effective Intervention

An effective response to cyberbullying requires a structured, balanced, and victim-centred approach. Interventions should prioritise emotional safety, confidentiality, fairness, and safeguarding considerations while ensuring that all actions remain proportionate to the nature and severity of the incident. Responses characterised by empathy, professionalism, and consistency contribute significantly to restoring trust and reducing further harm. Professionals should avoid minimising online harassment or treating cyberbullying as a less serious form of abuse simply because it occurs within digital spaces. Online incidents may produce consequences comparable to, or even more severe than, face-to-face bullying due to their permanence, public visibility, and potential to reach wide audiences rapidly.

Initial Response and Immediate Safety

The first stage of intervention should focus on ensuring the immediate emotional and psychological safety of the young person affected. A calm, respectful, and supportive environment is essential in allowing individuals to describe their experiences openly and without fear of judgment. Young people experiencing cyberbullying should receive reassurance that their concerns are being taken seriously and that responsibility for the abuse lies solely with those engaging in harmful behaviour. Professionals should assess whether the situation presents immediate safeguarding risks, including threats, coercion, hate speech, or indications of severe emotional distress requiring specialised support.

Information Gathering and Documentation

Accurate information gathering forms a crucial component of effective intervention. Professionals should allow young people to explain incidents in their own words while maintaining an attentive and non-judgmental approach. Clarification of facts should occur carefully and respectfully, without creating additional pressure or emotional discomfort.

Documentation of evidence represents an important protective measure. Screenshots, messages, emails, social media interactions, usernames, dates, and records of communication may assist institutions in understanding the situation fully and implementing appropriate procedures. Proper documentation also supports safeguarding responsibilities and may become necessary in situations involving legal or institutional escalation.

Assessing the Severity of the Situation

Not all cyberbullying incidents require identical responses. Effective intervention depends upon careful assessment of the severity, duration, frequency, and impact of the behaviour. Consideration should be given to whether the harassment involves repeated actions, coordinated group behaviour, discriminatory language, threats, dissemination of intimate material, or substantial emotional harm. This assessment assists professionals in determining the most appropriate course of action, including educational intervention, safeguarding procedures, parental involvement, referral to specialised services, or institutional disciplinary measures where necessary.

Implementing Appropriate Intervention Measures

Intervention measures should remain focused on protection, accountability, education, and behavioural improvement. Depending on the circumstances, responses may include restorative conversations, mediation processes where appropriate and safe, behavioural agreements, counselling support, digital safety guidance, or formal safeguarding actions. Educational approaches frequently contribute more effectively to long-term behavioural change than purely punitive responses. Young people involved in harmful online behaviour should be encouraged to understand the consequences of their actions, reflect upon emotional harm caused to others, and develop greater empathy and digital responsibility.

Monitoring and Follow-Up

Intervention should not conclude immediately after initial action has been taken. Ongoing monitoring and follow-up remain essential in ensuring that harmful behaviours have ceased and that affected individuals continue receiving appropriate support. Regular communication with the young person affected allows professionals to evaluate emotional well-being, assess ongoing risks, and strengthen feelings of safety and trust. Follow-up procedures additionally provide opportunities to monitor behavioural changes among perpetrators and evaluate the effectiveness of the intervention measures implemented. Sustained support and continued observation contribute significantly to long-term resolution and prevention of repeated incidents.

Supporting Victims and Addressing Perpetrators

Supporting Victims of Cyberbullying

Young people affected by cyberbullying require comprehensive and compassionate support that addresses emotional, psychological, social, and educational needs. Experiences of online harassment frequently generate feelings of shame, fear, isolation, helplessness, and loss of self-confidence. In many situations, victims may internalise blame or struggle to communicate the emotional impact of their experiences.

Supportive responses should therefore prioritise emotional reassurance, respectful communication, and the restoration of personal dignity and confidence. Professionals should create safe spaces where young people feel listened to, validated, and protected. Active listening, empathy, confidentiality, and emotional sensitivity remain essential throughout the support process. Where necessary, access to counselling services, psychological support, or safeguarding structures should be facilitated in order to ensure appropriate care and protection. Equally important is the encouragement of positive peer relationships, social participation, and re-engagement in educational or community activities that strengthen self-esteem and emotional resilience.

Recovery from cyberbullying extends beyond the cessation of abusive behaviour. Meaningful support involves helping young people rebuild trust, confidence, emotional stability, and a sense of belonging within their social and educational environments.

Addressing Perpetrators Through Educational Approaches

Effective intervention also requires appropriate engagement with those responsible for harmful online behaviour. While accountability remains essential, intervention strategies should additionally recognise the importance of education, reflection, and behavioural development. Young people who engage in cyberbullying may lack awareness regarding the consequences of their actions or may themselves experience emotional difficulties, peer pressure, insecurity, or previous experiences of victimisation. Understanding these contributing factors allows professionals to respond constructively while maintaining clear boundaries regarding unacceptable behaviour.

Educational and restorative approaches encourage perpetrators to reflect upon the emotional and social impact of their actions, recognise responsibility, and develop greater empathy toward others. Such approaches contribute more effectively to long-term behavioural change than responses based exclusively on punishment. Interventions may involve guided reflection, digital citizenship education, conflict resolution activities, awareness sessions, behavioural agreements, or individual support measures aimed at strengthening emotional intelligence and responsible online conduct.

Concluding Remarks

Cyberbullying represents a complex and evolving challenge requiring coordinated, informed, and compassionate responses from all professionals working with young people. Effective intervention depends upon timely identification, structured procedures, victim-centred support, and constructive educational engagement with those responsible for harmful behaviour. Through collaborative action, professional preparedness, and a strong commitment to safeguarding and inclusion, educational institutions, youth organisations, and community stakeholders can contribute significantly to the creation of safer, more respectful, and more supportive digital environments for young people across Europe.

PART 4 – Best Practices and Standardized Approach

Introduction to Part 4

The effective prevention and management of cyberbullying requires more than isolated actions or informal reactions to individual incidents. Sustainable impact depends upon clear institutional procedures, consistent professional practice, cooperation among relevant stakeholders, and a shared understanding of responsibilities. Cyberbullying is a complex phenomenon that affects the emotional well-being, social participation, educational experience, and digital rights of young people. Therefore, every organisation working with youth should be prepared to respond through structured, transparent, and child-centred mechanisms.

This part of the guide presents a standardised approach for institutions, youth organisations, educational settings, and community actors. It introduces an institutional response model, presents good practices and case study approaches from the partner countries, and outlines key policy and legal considerations relevant to cyberbullying prevention and response. The aim is to support professionals and institutions in developing coherent procedures that protect young people, strengthen accountability, and contribute to safer and more inclusive digital environments.

Institutional Response Model

An effective institutional response to cyberbullying should be based on preparedness, clarity, confidentiality, proportionality, and respect for the rights and dignity of every young person involved. Institutions should not approach cyberbullying as an isolated behavioural problem, but as a safeguarding, educational, and social inclusion concern that requires coordinated action.

The first element of an institutional response model is the establishment of a clear internal policy on cyberbullying and digital safety. Such a policy should define cyberbullying, describe unacceptable online behaviours, clarify reporting procedures, and explain the responsibilities of staff, young people, parents or guardians, and external partners. The policy should be accessible, age-appropriate, and communicated regularly to all members of the institutional community.

A second essential element is the creation of a safe and confidential reporting mechanism. Young people should be able to report cyberbullying without fear of blame, exposure, retaliation, or unnecessary escalation. Reporting procedures should allow incidents to be communicated to a trusted adult, designated safeguarding officer, youth worker, educator, or institutional representative. The existence of a clear reporting pathway increases trust and encourages early disclosure, which is essential for reducing harm.

Once an incident is reported, the institution should proceed with careful documentation and initial assessment.

The response should include the collection of relevant information, such as descriptions of the incident, digital evidence, dates, platforms involved, and the emotional impact on the young person affected. Documentation should be handled with discretion and in accordance with data protection principles. The purpose of documentation is not to create a punitive record, but to ensure accuracy, consistency, and informed decision-making.

The assessment stage should determine the severity of the incident and the level of risk involved. Particular attention should be given to cases involving threats, hate speech, sexual harassment, blackmail, non-consensual sharing of images, discrimination, repeated harassment, or serious emotional distress. Where safeguarding concerns arise, the institution should activate appropriate protection procedures and, where necessary, cooperate with specialised services or competent authorities.

The intervention itself should combine protection, support, accountability, and education. The young person affected should receive immediate emotional support and practical guidance. At the same time, the individual or group responsible for harmful behaviour should be addressed in a manner that promotes responsibility, reflection, and behavioural change. Disciplinary action may be necessary in serious cases, but educational and restorative measures should remain central whenever appropriate and safe.

The final stage of the institutional response model concerns monitoring and follow-up. Cyberbullying may continue after an initial intervention, particularly when digital content remains online or peer dynamics remain unresolved. For this reason, institutions should maintain communication with the young person affected, evaluate whether the harmful behaviour has stopped, and review whether additional support is required. Follow-up also allows the institution to assess the effectiveness of its own procedures and improve future responses.

A standardised institutional model ensures that responses are not dependent on individual judgement alone. It strengthens professional confidence, protects young people more effectively, and creates a culture of responsibility, trust, and digital respect.

Czech Best Practices

1. Safer Internet Center Czech Republic (SIC CZ)
https://bezpecnyinternet.cz/en/about-us/

Why it is considered a best practice

The Safer Internet Center Czech Republic (SIC CZ) is the national coordination platform promoting online safety and digital well-being for children and young people. Coordinated by CZ.NIC in cooperation with Safety Line, the Children's Crisis Centre, and JSNS (People in Need), the initiative combines prevention, education, counselling services, and a hotline for reporting illegal online content. SIC CZ provides comprehensive assistance to children, parents, educators, and schools.

As a member of the European Insafe and INHOPE networks, the Centre also contributes to international cooperation and the implementation of European online safety standards.

Key transferable elements
The initiative demonstrates the effectiveness of integrating prevention, counselling, victim support, and illegal content reporting within one coordinated national framework. It also highlights the importance of multi-stakeholder cooperation, combining educational institutions, non-governmental organisations, crisis support services, and international networks to strengthen online safety and digital resilience.

2. "Don't be a victim!" (Nebuď oběť!)
https://nebudobet.cz/

Why it is considered a best practice
"Don't Be a Victim!" (Nebuď oběť!) is a long-standing Czech educational initiative established in 2009 to promote the safe and responsible use of the internet and communication technologies. The programme focuses on the prevention of cyberbullying and other online risks through educational lectures, workshops, awareness campaigns, multimedia materials, and cooperation with schools across the Czech Republic. In addition to providing education for pupils, the initiative delivers accredited training for teachers and other professionals, actively cooperates with public institutions, law enforcement, and non-governmental organisations, and participates in national and international projects supporting online safety.

Key transferable elements
The project's comprehensive and community-based approach has contributed to raising awareness of cyberbullying and strengthening digital resilience among young people, educators, and the wider public.

3. "E-Safety" Project (Projekt E-Bezpečí)
https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu

Why it is considered a best practice
The E-Safety (E-Bezpečí) Project is a nationwide certified initiative dedicated to the prevention, education, research, intervention, and awareness-raising related to risky online behaviour. Implemented by the Centre for the Prevention of Risky Virtual Communication at Palacký University Olomouc, the project addresses cyberbullying, sexting, cyber grooming, cyberstalking, social media risks, fake news, online addictions, and other digital threats.

Key transferable elements
The project highlights the importance of combining research, education, prevention, counselling, and public awareness within a single long-term programme. Its multidisciplinary approach, extensive cooperation with educational institutions and public authorities, and continuous collection of research data provide a strong model for developing sustainable cyberbullying prevention strategies at both national and local levels.

Greek Best Practices

1. The Greek Safer Internet Centre (SaferInternet4Kids)

Why it is considered a best practice

The Greek Safer Internet Centre, coordinated by the Foundation for Research and Technology, Hellas (FORTH), constitutes one of the most comprehensive national initiatives addressing online safety, cyberbullying prevention, and digital literacy among children and young people. The initiative combines educational resources, awareness campaigns, training activities, helpline services, and evidence-based research aimed at strengthening digital resilience across educational communities. The Centre works directly with schools, educators, parents, and young people, offering practical tools and guidance for recognising and addressing cyberbullying incidents. Its integrated approach, combining prevention, awareness, support, and capacity-building, reflects the principles promoted by the European Better Internet for Kids (BIK+) strategy.

Key transferable elements

The success of this initiative demonstrates the importance of combining educational materials, support services, awareness campaigns, and stakeholder engagement within a single coordinated framework. It further highlights the value of continuous monitoring of online risks through national surveys and research activities

2. "Live Without Bullying" (KMOP)

Why it is considered a best practice

"Live Without Bullying" is a nationally recognised initiative developed by KMOP – Social Action and Innovation Centre. The programme provides free online counselling and mediation services for children, adolescents, parents, and educators experiencing bullying and cyberbullying incidents. A distinctive feature of the initiative lies in its accessibility and emphasis on early intervention. Through online counselling, professional guidance, and mediation procedures, the programme supports both victims and those involved in bullying behaviours while promoting constructive conflict resolution and emotional well-being. The initiative has become an important reference point for community-based responses to bullying and cyberbullying in Greece.

Key transferable elements

The programme demonstrates the effectiveness of accessible support mechanisms, confidential counselling services, and restorative approaches that focus on communication, support, and behavioural change rather than solely punitive responses.

3. The TABBY Project (Threat Assessment of Bullying Behaviour in Youth)

Why it is considered a best practice

The TABBY Project represents one of the most extensively researched cyberbullying prevention initiatives implemented in Greece. Developed through European cooperation and applied within Greek schools, the programme combines awareness-raising, risk assessment, educational activities, and teacher involvement to identify and prevent cyberbullying behaviours among adolescents.

Research evaluating the programme demonstrated reductions in cybervictimization and improvements in awareness regarding online risks and responsible digital behaviour. The evidence-based nature of the intervention has contributed to its recognition as a successful prevention model within educational settings.

Key transferable elements
The programme highlights the importance of evidence-based interventions, systematic risk assessment, active student participation, and teacher training as components of comprehensive cyberbullying prevention strategies.

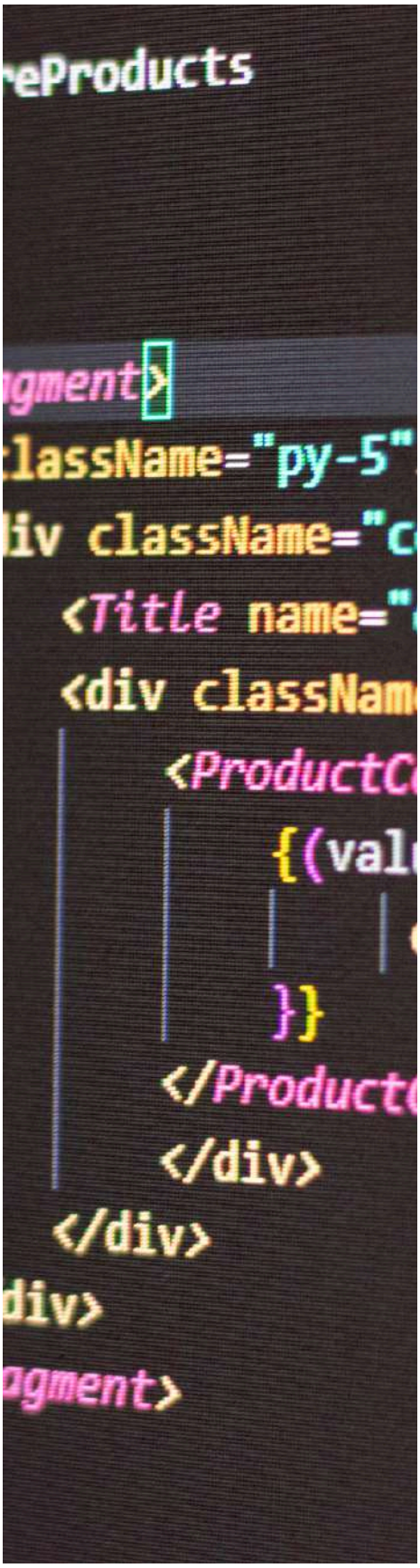
4. National Digital Platform Against School Bullying (stop-bullying.gov.gr)
Why it is considered a best practice
A significant recent development in Greece has been the establishment of the national digital platform for reporting and managing school bullying incidents under Law 5029/2023. The platform enables students and parents to report incidents while providing schools with structured procedures for documentation, intervention, monitoring, and follow-up. The initiative introduces a standardised national framework for addressing bullying and cyberbullying, strengthening institutional accountability and ensuring consistent responses across educational settings. The platform also supports teacher training and coordination among educational stakeholders.

Key transferable elements
This initiative illustrates the value of standardised reporting procedures, institutional coordination, digital monitoring systems, and clearly defined intervention protocols for ensuring consistent and effective responses to bullying incidents.



Bulgarian Best Practices

Bulgaria has a meaningful but still fragmented prevention and response ecosystem for cyberbullying. The strongest parts of the system are the Ministry of Education and Science's school-safety framework, the State Agency for Child Protection's national child-protection mechanisms, the Bulgarian Safer Internet Centre's helpline and hotline infrastructure, and a growing set of school-based whole-school programs such as **Steps Together** and **Online Safety School**. The weakest parts are the absence of a **standalone anti-cyberbullying law**, limited government-wide coordination on children's digital well-being, and weak national monitoring and evaluation of what actually reduces online harm over time. The 2025 Better Internet for Kids country profile for Bulgaria explicitly notes that there are **no national or regional laws, regulations or policies specifically in place to protect children from cyberbullying**, and it also identifies gaps in national coordination, monitoring, and dedicated research funding for children's digital environment.



The Bulgarian legal framework therefore works mostly through overlapping routes rather than a single cyberbullying statute. Depending on the facts, a case may engage child-protection duties, school procedures, police/cybercrime response, data-protection remedies, anti-discrimination remedies, or criminal-law provisions concerning threats, insult, defamation, coercive behaviour, intimate-image abuse, or other unlawful online conduct. Schools operate under the Mechanism for Combating Bullying and Violence in Institutions in the System of Preschool and School Education, while child-protection bodies may be triggered whenever a child is at risk. The State Agency for Child Protection states that anyone who becomes aware that a child needs protection must notify the Social Assistance Directorate, SACP, or the Ministry of the Interior immediately.

The evidence base shows the problem is material. A UNICEF-commissioned national study found that 10.9% of children and young people reported prior online abuse/bullying, most often on social media, and parents reported online bullying in 14% of cases. UNICEF's later regional reporting also described cyberbullying as affecting around 15% of children in Bulgaria, while broader school-violence indicators remain elevated. Bulgaria also continues to lag on basic digital skills compared with many EU peers: NSI reported that in 2025, 52.8% of 16–24-year-olds had basic or above-basic digital skills. These are not the same indicator sets, but together they show a policy challenge that spans safety, reporting confidence, and digital competence.

The most evidence-based strategy for Bulgaria is a **two-year whole-school implementation model** rather than one-off awareness events. That conclusion fits both international evidence and Bulgarian program experience. Systematic reviews and meta-analyses show that anti-cyberbullying programs are more effective when they combine teacher training, social-emotional learning, peer participation, clear reporting mechanisms, and family engagement. Bulgaria's **Steps Together** progress report similarly states that visible school-level results emerge after **at least two school years** of structured work, with mentoring support and full-school participation.

For implementation, the most practical option—assuming no fixed budget has been specified—is a staged rollout: start with governance, reporting, and baseline measurement; then train staff and peer mentors; then embed regular lessons and family engagement; then evaluate and scale. A realistic **core per-school cost** for a two-year program in Bulgaria is approximately **€12,000–€30,000**, rising to **€30,000–€60,000** for an enhanced model with more counseling time, external mentoring, and stronger evaluation. These are analytic estimates, not official tariffs, and they are based on Bulgaria's education-wage benchmarks and the scale of current public anti-violence funding windows. Bulgaria's 2025 EU-funded school violence-prevention call had a total budget of **35 million BGN** (about **€17.9 million**) and a cap of **350,000 BGN** per project (about **€179,000**), which makes cluster-based and municipal-scale implementation feasible.

What the Evidence Shows in Bulgaria

Bulgaria has credible recent data, but it is spread across UNICEF studies, HBSC analyses, Safer Internet Centre operational data, and sectoral reports rather than a single national observatory. A key national baseline is UNICEF Bulgaria's 2021 violence-against-children study, which found that more than **one in ten** children and young people reported prior online abuse, that the most common perpetrators were other children known to the victim, and that social-media sites were the most frequently reported location. The same report also found that girls were more likely to report stalking-like experiences, while some ethnic minority children reported significantly higher exposure to those experiences.

A later UNICEF regional update reported that around **15%** of children in Bulgaria experience cyberbullying, while school peer violence and bullying remain common more broadly. That matters because cyberbullying in practice often overlaps with school bullying rather than replacing it. International research also shows this overlap clearly: anti-bullying interventions work best when they address the student relationship climate as a whole rather than treating "online" and "offline" harm as entirely separate silos.

Bulgarian adolescent data also point toward protective factors. A 2022 study using the Bulgarian **HBSC 2017/2018** dataset found that bullying, cyberbullying, and physical fighting were prevalent among 15-year-olds and were more common among boys, while Positive Youth Development characteristics were protective. That is important for prevention design in Bulgaria because it supports moving beyond purely punitive approaches toward competence, confidence, connection, character, and caring—elements that map well onto social-emotional learning and peer-support models already embedded in current Bulgarian programs.

A second core risk factor is digital capacity. NSI reported in 2025 that **38.3%** of individuals in Bulgaria had basic or above-basic digital skills overall, and **52.8%** of young people aged 16–24 did so.

That is a significant improvement area for a country trying to reduce online harms among children and adolescents. Prevention in Bulgaria therefore should not be framed only as "behaviour control"; it also needs to build children's practical digital judgment, parental mediation skills, platform-reporting fluency, and evidence preservation habits. One final evidence point is negative rather than positive: Bulgaria still lacks strong national-level monitoring of children's digital well-being. The 2025 Better Internet for Kids policy monitor says there is no government-level system for gathering information on children and the digital environment, no systematic monitoring and evaluation of policies in this area, and no dedicated national coordination mechanism. That gap is central. It means Bulgaria already has useful programs, but it still does not have a robust state-level learning loop telling policymakers which interventions reduce harm most efficiently.

Legal Framework and Enforcement in Bulgaria

Bulgaria does not currently appear to have a standalone cyberbullying statute or a single national anti-cyberbullying act. Instead, harmful online conduct involving children is handled through multiple legal and administrative pathways. The table below shows the most relevant routes.



Instrument or route	What it covers in practice	Main authority or authorities	Why it matters for cyberbullying prevention	Key source
Child Protection Act framework	Child-in-risk situations and immediate protection duties	SACP, Social Assistance Directorate, Ministry of Interior	Creates the duty to report when a child needs protection; essential for serious or repeated cyberbullying, coercion, sextortion, or self-harm risk	SACP reporting page and institutional role pages

Instrument or route	What it covers in practice	Main authority or authorities	Why it matters for cyberbullying prevention	Key source
Mechanism for Combating Bullying and Violence in Preschool and School Education	School procedures, internal response levels, coordination council, annual reporting	MOES, Regional Education Authorities, schools	This is the most operational school-level anti-bullying instrument in Bulgaria; it explicitly recognises cyberbullying as especially humiliating because it is hard to stop and reaches a larger audience	Official MON/RUO documents
Preschool and School Education Act and inclusive-education rules	Safe school environment, support, sanctions, and personal-development support	MOES and schools	Gives the legal basis for school rules, support plans, participation of parents, and institutional duties	ZPUO / inclusive-education references
Criminal Code routes	Threats, coercive behaviour, insult/defamation-type harms, intimate-image abuse, computer-linked offences depending on facts	Police, prosecutors, courts	Bulgaria uses ordinary criminal-law tools rather than a cyberbullying-specific offense; BIK also states intimate-image abuse is covered by the Criminal Code	BIK profile, Lex references to private-complaint route and offense framework

Instrument or route	What it covers in practice	Main authority or authorities	Why it matters for cyberbullying prevention	Key source
Personal Data Protection Act and GDPR	Unlawful processing/sharing of personal data, images, videos, school or platform data misuse	Commission for Personal Data Protection	Important where cyberbullying includes non-consensual image sharing, doxxing, unlawful disclosure of identifying data, or excessive processing by institutions	CPDP official pages
Protection against Discrimination Act	Harassment or unequal treatment based on protected characteristics	Commission for Protection against Discrimination	Important when cyberbullying is discriminatory—e.g., anti-Roma, disability-based, homophobic, sexist, religious, or ethnic harassment	CPD official pages
Digital Services Act implementation in Bulgaria	Platform obligations, complaint pathways, transparency, illegal-content reporting	CRC as DSA coordinator; CEM for video-sharing/service areas; European Commission for VLOPs/VLOSEs	Relevant to platform reporting, user rights, and systemic-risk mitigation for minors; useful for structural prevention and accountability	CRC and EC pages

The most important operational point is that **Bulgaria's response is multi-track**. Schools should not wait for criminal qualification before acting. If a case involves humiliation, pile-on harassment, fake accounts, image-based abuse, school-group chat targeting, or discriminatory harassment, the school route, child-protection route, platform route, and—where necessary—police or data-protection route can all run in parallel. That is consistent with Bulgarian child-protection obligations and with the school mechanism's graded-response model.

Enforcement agencies and recent public examples

The main enforcement and remedy bodies are:

- **Ministry of Interior / GDBOP Cybercrime Directorate**, including online reporting through the cybercrime portal and police action where conduct reaches criminal or urgent-risk thresholds.
- **State Agency for Child Protection**, which coordinates child-rights protection nationally and runs the national children's helpline **116 111**.
- **Social Assistance Directorates / child-protection units**, which must be notified where a child needs protection.
- **Commission for Personal Data Protection**, for privacy and unlawful data-sharing elements.
- **Commission for Protection against Discrimination**, where a harassment pattern is discriminatory.
- **Ombudsman of the Republic of Bulgaria**, as a child-rights and complaint institution when public bodies have failed to protect rights.
- **Prosecutor's Office**, for criminal investigations and case progression.

Publicly searchable Bulgarian case law that is explicitly indexed under "cyberbullying" is limited. In practice, the public official record is more often published as police, prosecutor, Ombudsman, or regulator notices about online threats, image abuse, child sexual exploitation, scams, or harmful online conduct. That is a limitation of the public evidence base and should be acknowledged up front. The most visible recent official examples are these:

Recent public example	Why it matters	Source
In November 2025, GDBOP reported **276** signals linked to online sexual exploitation of children from the start of 2025, **33** specialized police operations, and identification of **113** children with risky online behaviour; the same notice lists cyberbullying among the major online threats to children.	Shows that cyberbullying prevention in Bulgaria cannot be separated from wider online child-protection and image-based abuse risks.	
In a 2025 GDBOP prevention event in Razgrad, officers told students that GDBOP receives **100–150 signals per day** relating to scams, extortion, and cyberbullying, and advised preserving screenshots as evidence.	Useful operational guidance: stop contact, preserve evidence, escalate.	
In June 2025, the Ombudsman alerted GDBOP, MOES, SACP, and the Parents Association about a harmful online game and dangerous computer viruses spreading in schools.	Shows that the Ombudsman can function as an escalation and rights-protection institution in digital child-safety issues affecting schools.	

A final legal-development point is the Digital Services Act. In May 2025, the European Commission sent Bulgaria a reasoned opinion for failing to empower a Digital Services Coordinator and set penalties under the DSA. By mid-2026, however, the Bulgarian Communications Regulation Commission publicly presents itself as the coordinator/competent authority for DSA implementation and provides DSA complaint information. For cyberbullying prevention, this matters because it creates a more realistic path for structural complaints about platform reporting, transparency, notice-and-action systems, and minors' protection.

Policy, Curriculum, Programs, and Reporting Channels
National policy and curriculum landscape

At the strategic level, the Strategic Framework for the Development of Education, Training and Learning in the Republic of Bulgaria 2021–2030 puts strong emphasis on cohesive school communities, work with parents, inclusion, digital transformation, and innovation. It is not a cyberbullying strategy by itself, but it is the umbrella under which current school-safety and digital-transformation work sits. In parallel, SACP's National Programme for the Prevention of Violence and Abuse of Children 2023–2026 and the 2025–2026 action plan provide the national child-protection frame, while the Council of Ministers formally adopted the 2025–2026 action plan by Decision No. 363 of 6 June 2025.

In curriculum terms, Bulgaria does not appear to teach "cyberbullying" as a universal standalone subject. Instead, it is addressed through a combination of:

computer modelling and information technology in lower grades, broader digital competencies and safe internet use in IT curricula, civic education grounded in rights frameworks, school class meeting and preventive activities, and targeted methodologies supplied through SafeNet, UNICEF, and MOES-approved or MOES-supported resources. MOES materials explicitly state that internet safety is an important component of the V–VII computer modelling and IT curricula, and the IX grade IT curriculum is framed around students' digital competencies. Civic education in XII grade is based on human-rights instruments including the Convention on the Rights of the Child and the ECHR.

The practical implication is clear: for Bulgarian schools, the best practice is integration plus repetition, not one annual lecture. Cyberbullying prevention should appear in several places over the school year: classroom norms, digital skills lessons, civic and rights education, peer-support work, and parent engagement. That also matches the international evidence base on program effectiveness.

Major government and NGO programs
The most relevant Bulgarian programs are compared below.



Program or mechanism	Lead bodies	Current scale or status	What it contributes	Source
Mechanism for Combating Bullying and Violence	MOES / Regional Education Authorities / schools	System-level procedural framework	Defines levels of response, requires institutional policy alignment, coordination council, and annual reporting	
Steps Together	UNICEF Bulgaria + MOES	Piloted in 5 schools in 2020–2022; evaluation and scaling since 2023	Whole-school approach, mentoring, social-emotional learning, peer support, parent engagement; pilot results became visible after at least two school years	
Online Safety School	UNICEF Bulgaria + MOES + Regional Centres for Inclusive Education Support	Will reach **100 schools** over two academic years; **50 trained mentors**	Direct cyberbullying and online-safety implementation inside the Steps Together framework; school-led campaigns for ages **12–14** and **15–18**	
Bulgarian Safer Internet Centre / SafeNet	Association Roditeli-led consortium; part of Insafe/INHOPE ecosystem	Ongoing national infrastructure	Helpline **124 123**, online chat, reporting hotline, teacher and parent resources, digital/media literacy, youth panel, Cyberscouts	
Cyberscouts	SafeNet / ARC Fund and partners	Youth-led peer education	Trained students aged **11–13** to educate peers on digital risks; complements mentor-led models	
National Programme Security	MOES	2025 national programme	Includes a cyber-security module on personal-information protection, password security, online threats and social engineering	
National Programme Without Aggression for a Safe Educational Environment	MOES	2025 programme implemented in **52 schools** and **28 kindergartens**; Steps Together parent support embedded	Builds broader anti-aggression and safe-environment capacity; important for scaling parent involvement and SEL	
EU-funded school violence-prevention call BG05SFPR001-1.010	Executive Agency Programme for Education / MOES	2025 call; budget **35m BGN**; up to **350,000 BGN** per project; projects up to 36 months and through **31 Dec 2029**	Practical financing route for municipalities and large rollouts	

Two analytical conclusions follow from this map. First, Bulgaria already has implementable models; it does not need to invent them from scratch. Second, the biggest gap is not "absence of activity," but rather insufficient alignment and measurement across school, child-protection, and digital-safety systems.

Reporting mechanisms and hotlines in Bulgaria

Bulgaria's reporting landscape is comparatively strong if schools and families know how to use it. The weakness is awareness and coordination, not the complete absence of channels.

Channel	Best use case	Availability noted in source	What to do there	Source
112	Immediate danger, threats of violence, ongoing extortion, imminent self-harm, criminal emergency	Emergency line	Use when there is immediate danger or urgent police response is needed	
116 111 National Child Helpline	Any child-in-risk concern, advice, protective escalation	SACP describes it as free, 24/7, nationwide	Children and adults can seek advice or report a child at risk	
SafeNet 124 123	Non-emergency online harms involving children: cyberbullying, sextortion, impersonation, harmful content, panic, advice needs	Free national helpline; chat and report form also available	Get counseling, triage, and referral; use especially for online bullying and digital harms affecting children	
SafeNet online chat and report form	When the child or parent is more comfortable writing than calling	Available on SafeNet site	Send evidence, describe the incident, request help or takedown support	
Cybercrime.bg / MVR cybercrime reporting	Criminal or quasi-criminal online acts: extortion, account takeover, image-based abuse, persistent threats, fraud, impersonation with harm	Online reporting route	Report cybercrime and internet threats; preserve screenshots and metadata first	
SACP online signal form	Child-protection concerns and escalation where a child needs protection	Online signal channel	Report concerns and attach files; suitable when school or family needs child-protection intervention	
CPDP complaint	Doxxing, unlawful image/video sharing, misuse of personal data	Official complaint/alert route	Use where the harm includes unlawful data processing or exposure	
CPD complaint	Bias-based harassment or discriminatory cyberbullying	Official complaint route	Use for harassment linked to protected characteristics	
Ombudsman complaint	Rights failures by public bodies, school or institutional inaction	Electronic complaint form	Use when systems fail to protect a child's rights adequately	
School internal route	First-line response in most school-linked incidents	Institution-specific	Report to class teacher, school psychologist/counselor, deputy principal, or school coordination council	

For Bulgarian practice, the strongest reporting rule is this: preserve evidence before deletion whenever it is safe to do so. GDBOP explicitly advises victims to stop communication and keep screenshots as evidence for investigation. School policies should therefore instruct students and staff to capture enough evidence first, screen, URL, user handle, date/time, message history, witnesses, before blocking or reporting, unless there is an immediate safety risk.

Prevention Model for Families, Schools, Platforms, and Policymakers

Families and caregivers

For families in Bulgaria, prevention should emphasize active mediation, not only surveillance. The CPDP's official guidance for parents recommends setting clear rules for safe internet use, taking personal responsibility for children's online safety, and keeping internet access in shared spaces where possible. CPDP's child-facing advice adds the basics of not sharing personal information and being cautious with digital traces. These are useful foundations, but they are not sufficient on their own for adolescent cyberbullying prevention.

The stronger family practice is a short, repeatable routine: weekly check-ins; discussion of class/group-chat norms; explicit permission for the child to report before a situation becomes "serious"; a no-punishment rule for reporting embarrassing content; and a standing plan for what to do if intimate images, fake profiles, or public humiliation occur. In Bulgaria, parents should also know the exact external routes: 124 123, 116 111, 112, and cybercrime.bg. This matters because adolescents often delay disclosure when they expect blame or device confiscation. Bulgarian helpline infrastructure works only if young people believe adults will use it constructively.

A practical family segmentation is advisable because the user did not specify target age groups. The cleanest operational split is:

Age band	Best prevention emphasis
6–10	Device routines, privacy basics, trusted-adult disclosure, kind online behaviour
11–13	Group-chat norms, fake accounts, image sharing, early peer pressure, Cyberscout-style peer education
14–18	Sextortion, intimate-image abuse, reputational harm, legal consequences, platform reporting, evidence preservation

This age segmentation is a recommended implementation option, not a binding Bulgarian standard. Some Bulgarian programs specify ages, for example Cyberscouts at 11–13, SafeNet youth participation at 14–18, and the Online Safety School competition at 12–14 and 15–18—but not all national materials use the same brackets.

Schools, platforms, and policymakers
For schools, the Bulgarian best-practice model is now clear. It is the whole-school approach: leadership commitment, staff training, clear internal procedures, peer support, parent involvement, and repeated student work on digital empathy and conflict handling. The Steps Together program states this directly, and its progress report says pilot schools showed significant changes in school environment and cohesion, with visible results appearing after at least two school years. That means schools should avoid treating cyberbullying as a one-day campaign topic. It is a culture issue and a system issue.

For platforms operating in Bulgaria, the right approach is DSA-compliant moderation adapted to Bulgarian user pathways. Meta's help center says users can report bullying and harassment on Instagram and Facebook; TikTok states it removes bullying, degrading or harassing behaviour and takes a particularly strong line on bullying affecting children; YouTube has harassment and cyberbullying policies and publishes enforcement information through its transparency reporting. Under the DSA and the Commission's minors guidelines, platforms used by Bulgarian children should provide easy reporting, age-appropriate design, and effective mitigation of risks to minors. In the Bulgarian context, this should translate into: Bulgarian-language reporting and safety pages; easy routes for reporting fake profiles, doxxing, humiliating edits, intimate-image abuse, and pile-on harassment; in-app signposting to 124 123, 116 111, or 112 when risk is acute; and operational cooperation with the Bulgarian Digital Services Coordinator and child-safety actors when systematic harms are identified.

For policymakers, the priority is not to add another isolated awareness campaign. T

he priority is to close the system gaps identified in Bulgaria itself: no strong national coordination mechanism, no integrated government-level data system on children's digital environment, and no reliable monitoring of policy outcomes. The most valuable reforms would therefore be: a national indicator set; a reporting-data protocol shared by MOES, SACP, SafeNet, and MVR; confidential complaint mechanisms in schools; ongoing capacity-building for judges, prosecutors, police, and educators; and stable financing for school-based two-year implementations. These recommendations are closely aligned with the UN Committee on the Rights of the Child's 2024 observations on Bulgaria, which called for confidential child-friendly complaint mechanisms in schools and capacity-building for judges, prosecutors, police, and other professionals.

Metrics, Implementation Plan, and Practical Tools

What to measure and how to judge success

Bulgaria should measure effectiveness at four levels: prevalence, response quality, school climate, and capacity. Because national monitoring is currently weak, schools and municipalities should build their own local dashboards from day one. That is more useful than waiting for a perfect national system.

Metric	Why it matters	Suggested source	Cadence	Good target after 2 school years
Cybervictimization in past 2 months	Core outcome	Anonymous student survey aligned to HBSC wording	Baseline, 12 months, 24 months	**10–25% relative reduction** from baseline, adjusted for reporting effects
Cyberbullying perpetration in past 2 months	Core behaviour outcome	Anonymous student survey	Baseline, 12 months, 24 months	**10–20% relative reduction**
Student knowledge of where to report	Capacity and access	Pulse survey	Termly	**85%+** can name at least 2 correct routes
Median time from report to school triage	Response quality	Case log	Monthly	**<48 hours** for non-emergency cases
Share of serious cases escalated correctly	Child-protection quality	Case audit	Quarterly	**90%+** protocol compliance
Repeat victimization within 90 days	Recovery quality	Case follow-up	Quarterly	Downward trend year-on-year
Staff trained and refreshed	Institutional capacity	HR/training records	Termly	**90%+** staff trained annually
Parent participation rate	Family engagement	Attendance records	Termly	**40–60%** in first year; improve thereafter
School climate / belonging / perceived safety	Protective factor	Student survey	Baseline, 12 months, 24 months	Statistically meaningful improvement
External referrals to 124 123 / 116 111 / platform / MVR where indicated	Use of system	Aggregated logs	Quarterly	Not "lower is better"; first-year increase may indicate better trust and awareness

The first-year interpretation must be careful. Better reporting often makes the numbers look worse before they get better. A rise in reported incidents during the first implementation year can actually be a positive signal if it is accompanied by faster triage, higher student trust, stronger evidence preservation, and lower recurrence. That is why Bulgaria needs both prevalence metrics and process metrics.

Recommended implementation steps, timeline, and estimated costs

The table below assumes no specific budget has been stated and uses a standard two-school-year implementation horizon because Bulgarian program evidence indicates that visible change usually requires at least that long. The cost ranges are analytic estimates based on Bulgarian education wage benchmarks published by NSI and the scale of public school-safety funding windows; they are not official government tariffs. NSI's preliminary 2025 average annual gross wage was 31,239 BGN (about €15,972) and the Q4 2025 average monthly wage was 2,678 BGN (about €1,369). Public anti-violence financing is also clearly in scope in Bulgaria, including the 2025 35 million BGN education call with 350,000 BGN per-project ceiling.

Phase	Timeline	Main actions	Indicative cost per school	Indicative cost for 10-school cluster	Notes
Preparation	Months 0–3	Adopt policy; appoint safeguarding lead; create coordination team; baseline student/parent/staff survey; map external contacts; prepare evidence-preservation protocol	**€2,000–€6,000**	**€20,000–€45,000**	Lowest-cost phase; mostly planning, training design, and baseline
Capacity building	Months 3–6	Train all staff; train peer mentors; parent briefings; create student-friendly reporting materials; platform-reporting playbooks	**€4,000–€10,000**	**€35,000–€90,000**	Use SafeNet/MOES/UNICEF materials where possible to cut cost
Core delivery	Months 6–12	Class meetings and lesson modules; peer-support work; restorative response pathways; case logging; referral network in use	**€4,000–€9,000**	**€40,000–€90,000**	First-year incident reports may rise as trust improves
Deepening and targeted support	Months 12–18	Intensive work with repeat cases, high-risk cohorts, class climates, and families; additional mentor visits	**€2,000–€8,000**	**€20,000–€80,000**	Higher end if external psychologist/mentor support is added
Evaluation and scale decision	Months 18–24	Repeat survey; case audit; student focus groups; public dashboard; scale-up plan or corrective plan	**€1,500–€5,000**	**€15,000–€50,000**	External evaluation is strongly recommended

Estimated two-year total per school:

Core model:** **€12,000–€30,000
Enhanced model:** **€30,000–€60,000
Estimated two-year total for a 10-school municipal cluster:

€120,000–€355,000, with the higher end approaching or exceeding the per-project ceiling in the 2025 education call, so large-scale clusters may need multiple funding lots, municipal co-financing, or phased procurement.

Estimated national rollout for 100 schools over two school years:
€1.2 million–€3.5 million for school delivery, plus €200,000–€500,000 for central coordination, communications, common survey tools, national evaluation, and translation/adaptation work. This is well within the same order of magnitude as Bulgaria's recent public funding windows for school-violence prevention.

Sample school cyberbullying policy template
The template below is an illustrative model aligned with the MON anti-bullying mechanism, the whole-school principles of Steps Together, and the child-rights emphasis on confidential complaint mechanisms. It should be adapted by each school to its legal counsel, internal regulations, and student age profile.

School Cyberbullying Prevention and Response Policy
Purpose
This policy aims to prevent, detect, respond to, document, and review cyberbullying affecting students, including incidents that begin outside school but substantially affect safety, learning, attendance, or well-being inside school.

Scope
Applies to students, staff, volunteers, and school-organized digital spaces, and to off-campus digital conduct where there is a clear school impact. If target age group is not yet defined, the school should explicitly state whether the policy applies to all grades or to a pilot band only.

Definition
Cyberbullying includes repeated or severe harmful conduct using digital tools, such as humiliating messages, fake accounts, image-based abuse, exclusion from online groups, doxxing, threats, coercive contact, disclosure of personal data, or discriminatory harassment. School policy should note that a single severe act may justify immediate protective action. This broader definition is consistent with current scientific recommendations that bullying definitions be inclusive of severe harm and digital dynamics.

Reporting routes
Students and adults may report to: class teacher, school psychologist/counselor, deputy principal, principal, or designated safeguarding lead. External routes must be listed in the appendix: **124 123**, **116 111**, **112**, **cybercrime.bg**, platform reporting tools, SACP, CPDP, CPD, and Ombudsman as appropriate.

Immediate safety response
If there is immediate danger, sexual extortion, intimate-image abuse, suicidal intent, credible threat of violence, or stalking, the school escalates immediately to the emergency and child-protection routes and documents the time of each action.

Evidence preservation
Before deleting content, the school supports the student or parent in capturing screenshots, links, usernames, dates, times, and the names of witnesses, unless doing so creates immediate additional danger.

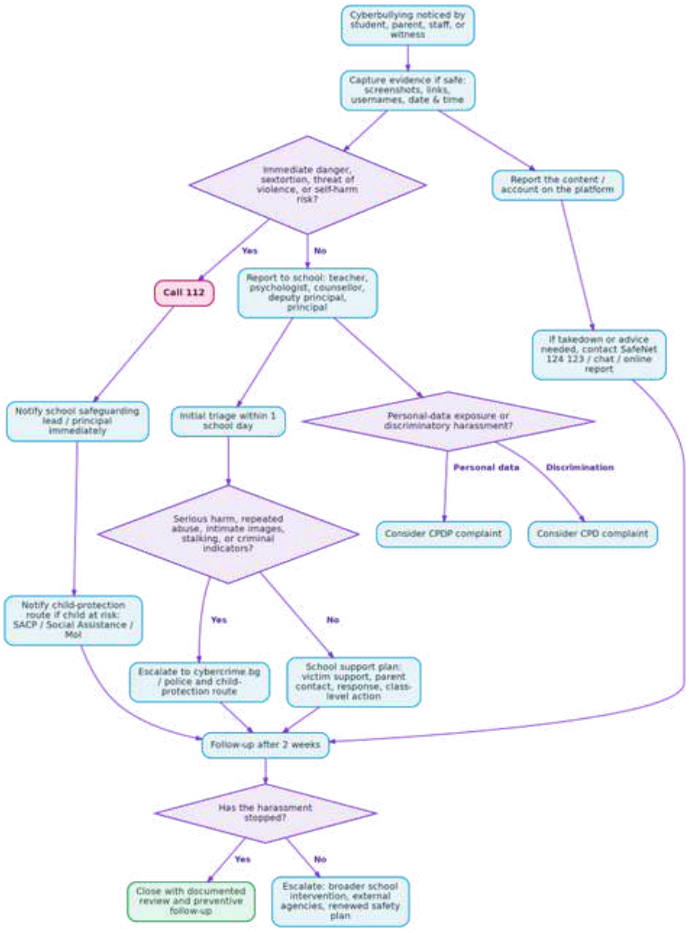
Response timeline
Initial triage within one school day; contact with parents or guardians within one to two school days where appropriate; formal case plan for serious incidents within three school days; follow-up review after two weeks and again after one to three months. This is a best-practice target, not a statutory Bulgarian deadline. It should be written into the school's own procedures.

Interventions
Use graduated responses: supportive conversation, class-level work, restorative process where safe, counselling, parent conference, behaviour plan, platform reporting, temporary digital restrictions in school systems, referral to child-protection or police, and disciplinary measures where required by law and school rules. Evidence shows this layered approach works better than one-off punishment alone.

Special protections
Cases involving disability, ethnicity, religion, sex, sexual orientation, gender expression, language, migrant background, or any protected characteristic must be screened for discriminatory harassment and, where applicable, referred to the Commission for Protection against Discrimination. Cases involving personal-data exposure must be screened for CPDP referral.

Record keeping and review
The coordination team keeps anonymized aggregate data on reports, response times, recurrence, and outcomes and presents an annual review to school leadership. This aligns with the MON mechanism's emphasis on institutional reporting and annual recommendations for a safer educational environment.

Sample reporting flowchart
The flow below is designed for Bulgarian schools and families and combines internal school handling with Bulgarian external reporting channels.



This flow is consistent with Bulgarian child-protection reporting duties, the school anti-bullying mechanism, SafeNet's helpline/hotline role, and GDBOP's advice on preserving evidence.

Analytical bottom line

For Bulgaria, the strongest path is not a brand-new standalone campaign. It is an **integrated national-to-school architecture** that uses what already exists and fixes what is missing. That means:

1. make every school's policy and referral map operational and student-friendly;
2. embed cyberbullying content into repeated curriculum and class-meeting practice;
3. scale whole-school models like **Steps Together** and **Online Safety School** rather than one-off talks;
4. standardize data capture across schools, SafeNet, SACP, and MVR;
5. use DSA-era leverage to push platforms toward more accessible, child-centered reporting and response for Bulgarian users; and
6. fund interventions for **at least two school years**, because that is when Bulgaria's own evidence says change becomes visible.

If the target age group, school level, municipality size, or delivery model is still unspecified, the most practical next-step options are: **single-school pilot**, **10-school municipal cluster**, or **100-school regional/national cohort**. The evidence supports all three, but the best value-for-money in the Bulgarian system is likely the **cluster model**, because it allows shared training, referral protocols, evaluation, and mentorship while staying close enough to schools for implementation discipline.

Policy and Legal Considerations

Cyberbullying represents a significant challenge that extends beyond interpersonal conflict and increasingly requires coordinated educational, institutional, policy, and legal responses. As digital technologies continue to shape communication, learning, and social participation among young people, the protection of children and adolescents within online environments has become a growing priority at both European and international levels. Educational institutions, youth organisations, policymakers, and digital platforms all share responsibility for ensuring that young people are able to participate safely, respectfully, and confidently within digital spaces.

Cyberbullying is closely connected to issues of human rights, child protection, privacy, dignity, emotional well-being, equality, and digital citizenship. Harmful online behaviour may include harassment, intimidation, discrimination, hate speech, impersonation, exclusion, threats, stalking, or the non-consensual sharing of private content. Such behaviours can produce serious emotional, psychological, social, and educational consequences for young people and therefore require comprehensive and structured responses grounded in safeguarding principles and respect for fundamental rights.

At international level, organisations such as UNICEF, UNESCO, and the Council of Europe have consistently emphasised that children and young people possess the right to protection from all forms of violence, including violence occurring in digital environments. The Council of Europe highlights that digital environments should safeguard the dignity, privacy, security, and well-being of children while promoting safe participation and responsible online engagement. Similarly, UNESCO stresses the importance of whole-school and whole-community approaches that integrate prevention, awareness, support, and intervention mechanisms within educational settings.

Within the European Union, digital safety and the protection of minors online have become central policy priorities. The Better Internet for Kids (BIK+) strategy promotes safer and more empowering digital experiences for children and young people, focusing on digital literacy, online participation, protection from harmful content, and responsible use of digital technologies. In parallel, the Digital Services Act introduces obligations for online platforms and digital service providers to strengthen privacy protections, reduce exposure to harmful online content, and implement safety measures for minors. These developments demonstrate a broader recognition that cyberbullying cannot be addressed solely through individual action, but requires cooperation between educational institutions, public authorities, digital platforms, families, and civil society organisations.

From an institutional perspective, schools, youth organisations, and educational bodies should establish clear and accessible policies concerning cyberbullying prevention and response.

Institutional policies should define unacceptable online behaviours, clarify reporting procedures, explain safeguarding obligations, and outline intervention measures. Such policies should also establish clear roles and responsibilities for educators, youth workers, management staff, young people, parents or guardians, and external support services.

Effective institutional policies should prioritise prevention, education, and safeguarding rather than relying exclusively on disciplinary approaches. Awareness activities, digital literacy education, emotional well-being initiatives, and the promotion of respectful online communication represent essential components of comprehensive prevention strategies. Educational environments that encourage empathy, inclusion, diversity, and responsible digital participation contribute significantly to reducing harmful online behaviour and strengthening positive peer relationships.

Data protection and privacy considerations remain particularly important in cases involving cyberbullying. Reporting and intervention procedures frequently involve sensitive information, including screenshots, messages, images, usernames, and personal data related to minors. Institutions therefore carry responsibility for ensuring that all information is handled securely, confidentially, and in accordance with applicable data protection legislation, including the General Data Protection Regulation (GDPR). Access to sensitive material should remain limited to authorised individuals directly involved in the management and safeguarding process.

In situations involving threats, hate speech, discrimination, blackmail, stalking, identity misuse, or the non-consensual sharing of intimate content, institutions may be required to cooperate with child protection services, specialised support organisations, helplines, legal authorities, or law enforcement bodies. Clear referral pathways and safeguarding procedures are essential for ensuring appropriate responses in cases involving serious emotional harm, criminal behaviour, or risks to personal safety.

Across Europe, many countries have strengthened national strategies, educational frameworks, and reporting mechanisms related to bullying and cyberbullying prevention. Initiatives developed through Safer Internet Centres, digital literacy programmes, educational campaigns, helplines, and institutional reporting systems demonstrate increasing recognition of the need for coordinated and standardised responses. These initiatives further highlight the importance of cross-sector cooperation involving educators, youth workers, policymakers, families, researchers, digital experts, and young people themselves.

Policy and legal frameworks should ultimately support one central objective: the protection and empowerment of young people within digital environments. Effective policies contribute not only to the management of incidents, but also to the creation of educational cultures founded upon safety, inclusion, equality, respect, participation, and digital responsibility. Institutions that establish clear procedures, strengthen professional preparedness, encourage youth participation, and promote respectful digital behaviour contribute significantly to safer and more inclusive online communities across Europe. As digital environments continue to evolve, ongoing adaptation of policies, educational practices, and safeguarding mechanisms remains essential. Cyberbullying prevention should therefore be understood as a continuous process requiring cooperation, awareness, professional development, and long-term commitment from all stakeholders involved in the lives of young people.

PART 5 – Practical Tools

Resources

- 1. Academic Research and Scientific Literature
- Ahmed, S., et al. (2024). Cyberbullying research. International Journal of Educational Research Open. https://doi.org/10.1016/j.ijedro.2024.100341
- Daskalaki, E., Psaroudaki, K., Karkanaki, M., & Fragopoulou, P. (2020). Understanding the online behavior and risks of children: Results of a large-scale national survey on 10–18 year olds. arXiv. https://arxiv.org/abs/2008.10274
- Matos, A., et al. (2025). Cyberbullying and European educational policies. Social Sciences, 14(8), Article 505. https://doi.org/10.3390/socsci14080505
- Melista, T. (2025). Integrating legal mandates and social work in bullying prevention: The Greek model under Law 5029/2023. PubMed Central. https://pmc.ncbi.nlm.nih.gov/articles/PMC12617174/

2. European Union Institutions and Policy Documents

- Better Internet for Kids. (n.d.). Greece: Policy monitor country profile. European Schoolnet. Retrieved June 4, 2026, from https://better-internet-for-kids.europa.eu/en/knowledge-hub/greece-policy-monitor-country-profile
- Better Internet for Kids. (n.d.). Greek Safer Internet Centre. European Schoolnet. Retrieved June 4, 2026, from https://better-internet-for-kids.europa.eu/en/sic/greece
- European Commission. (2024). EU action plan against cyberbullying. Better Internet for Kids. https://better-internet-for-kids.europa.eu/en/news/eu-action-plan-against-cyberbullying
- European Commission. (2025). Cyberbullying survey results: Full report. https://eu-for-children.europa.eu/system/files/2025-11/Cyberbullying-Survey-Results-Full-Report_2025.pdf
- European Commission. (2025). Cyberbullying: Insights from science, policy and legislation (JRC144335). Publications Office of the European Union. https://doi.org/10.2760/0941861
- European Commission. (n.d.). Cyberbullying. https://digital-strategy.ec.europa.eu/en/policies/cyberbullying
- European Commission. (2025). Better Internet for Kids (BIK) policy monitor: Bulgaria country profile. https://digital-strategy.ec.europa.eu
- European Commission. (2025). Digital Services Act: Protection of minors and reasoned opinion to Bulgaria. https://digital-strategy.ec.europa.eu

3. International Organisations and Reports

- Council of Europe. (n.d.). Bullying and cyberbullying. Retrieved June 4, 2026, from https://www.coe.int/en/web/children/bullying
- UN Committee on the Rights of the Child. (2024). Concluding observations on the combined sixth and seventh periodic reports of Bulgaria. United Nations.

- UNESCO. (2022). *The role of teachers in preventing and addressing school violence and bullying*. United Nations Educational, Scientific and Cultural Organization.
- UNESCO. (2024). *Bullying and cyberbullying: Guidance for education stakeholders*. United Nations Educational, Scientific and Cultural Organization.
- UNICEF. (2019). *Behind the numbers: Ending school violence and bullying*. United Nations Children's Fund. https://www.unicef.org/media/66496/file/behind-the-numbers.pdf
- UNICEF. (n.d.). *How to stop cyberbullying*. United Nations Children's Fund. Retrieved June 4, 2026, from https://www.unicef.org/stories/how-to-stop-cyberbullying
- UNICEF. (n.d.). *What to do if your child is experiencing cyberbullying*. United Nations Children's Fund. Retrieved June 4, 2026, from https://www.unicef.org/parenting/child-care/what-to-do-if-your-child-is-experiencing-cyberbullying
- World Health Organization Regional Office for Europe. (2024, March 27). *One in six school-aged children experiences cyberbullying, finds new WHO Europe study*. https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study

4. Greek National Authorities, Policies and Initiatives

- KMOP – Social Action and Innovation Centre. (n.d.). *Live Without Bullying*. Retrieved June 4, 2026, from https://livewithoutbullying.com
- Ministry of Education, Religious Affairs and Sports. (2023). *Law 5029/2023: Living together harmoniously – Breaking the silence. Regulations for the prevention and management of violence and bullying in schools and other provisions*. https://stop-bullying.gov.gr/institutional-framework
- Ministry of Education, Religious Affairs and Sports. (n.d.). *Stop-bullying.gov.gr: Special digital platform for the prevention and management of school bullying*. Retrieved June 4, 2026, from https://stop-bullying.gov.gr
- SaferInternet4Kids. (n.d.). *Help-Line: Support and counselling services for children, adolescents and families*. Foundation for Research and Technology – Hellas (FORTH). Retrieved June 4, 2026, from https://saferinternet4kids.gr/slider/γραμμή-βοηθείας-help-line/
- SaferInternet4Kids. (n.d.). *National awareness centre for the safe and responsible use of the internet*. Foundation for Research and Technology – Hellas (FORTH). Retrieved June 4, 2026, from https://saferinternet4kids.gr

5. Bulgarian National Authorities, Policies and Programmes

- Association Roditeli. (n.d.). Bulgarian Safer Internet Centre (SafeNet). https://www.safenet.bg
- Commission for Personal Data Protection. (n.d.). Official website. https://www.cpdp.bg
- Commission for Protection against Discrimination. (n.d.). Official website. https://www.kzd-nondiscrimination.com
- Communications Regulation Commission. (2025). Digital Services Act (DSA) coordination in Bulgaria. https://www.crc.bg
- Council for Electronic Media. (n.d.). Official website. https://www.cem.bg
- Executive Agency "Programme for Education." (n.d.). Call BG05SFPR001-1.010. https://sf.mon.bg
- Health Behaviour in School-aged Children. (2022). Positive youth development analysis: Bulgaria (Based on the 2017/2018 HBSC dataset). https://hbsc.org
- Ministry of Education and Science. (2021). Strategic framework for the development of education, training and learning in the Republic of Bulgaria (2021–2030).

- Ministry of Education and Science. (n.d.). Mechanism for combating bullying and violence in institutions in the system of preschool and school education. https://www.mon.bg
- Ministry of Education and Science. (n.d.). National Programme "Security". https://www.mon.bg
- Ministry of Education and Science. (n.d.). National Programme "Without Aggression for a Safe Educational Environment". https://www.mon.bg
- Ministry of Education and Science. (n.d.). Preschool and School Education Act (ZPUO). https://www.mon.bg
- Ministry of Interior, General Directorate Combating Organised Crime. (n.d.). Cybercrime Directorate. https://cybercrime.bg
- National Statistical Institute. (2025). Average wages and digital skills statistics. https://www.nsi.bg
- Ombudsman of the Republic of Bulgaria. (n.d.). Official website. https://www.ombudsman.bg
- State Agency for Child Protection. (2023). National Programme for the Prevention of Violence and Abuse of Children (2023–2026). https://sacp.government.bg
- State Agency for Child Protection. (2025). Action Plan for the National Programme for the Prevention of Violence and Abuse of Children (2025–2026). https://sacp.government.bg
- State Agency for Child Protection. (n.d.). National Child Helpline 116 111 and reporting procedures. https://sacp.government.bg
- UNICEF Bulgaria. (2021). Violence against children in Bulgaria: National study. https://www.unicef.org/bulgaria
- UNICEF Bulgaria. (n.d.). Online Safety School. https://www.unicef.org/bulgaria
- UNICEF Bulgaria, & Ministry of Education and Science. (n.d.). Steps Together programme.

6. Digital Platforms and Online Safety Resources

- Cyberbullying Research Center. (n.d.). Cyberbullying Research Center. https://cyberbullying.org
- Dianova International. (2024). Cyberbullying, the EU Digital Services Act and children's rights: Prevention and protection. https://www.dianova.org/news/cyberbullying-eu-digital-services-act-children-rights-prevention/
- Meta. (n.d.). Bullying, harassment and safety policies. https://transparency.fb.com
- TikTok. (n.d.). Safety Center. https://www.tiktok.com/safety
- YouTube. (n.d.). YouTube Safety Center. https://support.google.com/youtube

7. International Surveys and Public Opinion

- Pew Research Center. (2022, December 15). Teens and cyberbullying 2022. https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/





CyberGuard

Guide for Preventing and Combating Cyberbullying

CYBERGUARD

Learning Strategies for Preventing, Intervening, and Empowering Youth Against Cyberbullying

Project Number:
2025-1-CZ01-KA210-YOU-000365051

2026

PRINCEPS
RISK INTELLIGENCE INSTITUTE

fifty-fifty

EduAge

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the Czech National Agency for International Education and Research (DZS). Neither the European Union nor the granting authority can be held responsible for them.