

# Better Internet for Kids

## Classifying and responding to online risk to children

Good practice guide

February 2023

*Citation: Stoilova, M., Rahali, M. & Livingstone, S (2023) Classifying and responding to online risk to children: Good practice guide. London: Insafe helplines and the London School of Economics and Political Science (LSE).*



# Contents

<b>1. The guide</b> .....	<b>3</b>
<b>2. What is online risk to children?</b> .....	<b>4</b>
<i>i. Defining and classifying online risk to children</i> .....	4
<i>ii. Prevalence of online risk to children in Europe</i> .....	5
<b>3. Content risk: potentially harmful online content</b> .....	<b>6</b>
<i>i. Definition</i> .....	6
<i>ii. Prevalence</i> .....	7
a. Hate messages .....	8
b. Eating disorders.....	8
c. Ways to physically harm or hurt themselves.....	8
<i>iii. Case studies</i> .....	9
a. Malta .....	9
b. Greece .....	9
c. Lithuania .....	10
<i>iv. Resources</i> .....	10
<b>4. Contact risk: Online sexual coercion and extortion of children</b> .....	<b>11</b>
<i>i. Definition</i> .....	11
<i>ii. Prevalence</i> .....	12
<i>iii. Case studies</i> .....	12
a. Germany .....	12
b. Latvia.....	13
c. Bulgaria .....	13
<i>iv. Resources</i> .....	14
<b>5. Conduct risk: online reputation</b> .....	<b>15</b>
<i>i. Definition</i> .....	15
<i>ii. Prevalence</i> .....	15
<i>iii. Case studies</i> .....	16
a. Slovenia .....	16
b. Romania .....	16
c. Ireland .....	17
<i>iv. Resources</i> .....	17
<b>6. Contract risk: e-crime</b> .....	<b>18</b>
<i>i. Definition</i> .....	18
<i>ii. Prevalence</i> .....	19
<i>iii. Case studies</i> .....	19
a. Austria .....	19
b. Spain .....	19

c. Luxembourg .....20

iv. Resources.....21

**7. Conclusion .....21**

**Bibliography .....23**

**Annex I: Category definitions (BIK, 2023).....24**

**Annex II: Safer Internet Centre services and resources, by EU country .....26**

## Copyright notice

© European Union, 2023



The Commission's reuse policy is implemented by the [Commission Decision of 12 December 2011 on the reuse of Commission documents](#).

Unless otherwise indicated (e.g. in individual copyright notices), content owned by the EU within this publication is licensed under [Creative Commons Attribution 4.0 International \(CC BY 4.0\) licence](#). This means that reuse is allowed, provided appropriate credit is given and changes are indicated.

You may be required to clear additional rights if a specific content depicts identifiable private individuals or includes third-party works. To use or reproduce content that is not owned by the EU, you may need to seek permission directly from the rightsholders. Software or documents covered by industrial property rights, such as patents, trademarks, registered designs, logos and names, are excluded from the Commission's reuse policy and are not licensed to you.

# 1. The guide

**This guide sets out good practices by which professionals can respond constructively to the range of online risks of harm encountered by children in Europe. Its aim is to increase awareness of the risks and encourage the use of available tools and services to mitigate and remedy the resulting harms.**

Responding to policy and public concern regarding current and emerging online risks of harm to children in Europe, and grounded in research and practitioner expertise, the guide examines how online risks are classified, and the steps that children, caregivers, educators and Safer Internet Centres (SICs) can take to mitigate the resulting harms. This is illustrated by real-life case studies provided by SICs on contacts they have received and positive support they offered.

A thorough consideration of children's digital engagement requires attention to both online [opportunities](#) and risks, as part of a holistic approach to [children's rights in relation to the digital environment](#). To complement existing work on online opportunities – for example, the Better Internet for Kids (BIK) 2020 [good practice guide for positive online content](#) for children – and to harness professional knowledge to the serious societal need to strengthen child protection, this good practice guide focuses on online risk.

It is paramount that society's understanding of online risk is based on reliable research conducted with and in relation to children. Rather than imposing a vision grounded in adult assumptions, popular anxieties or media headlines, this good practice guide is informed by children's views, up-to-date empirical research by [EU Kids Online](#) and others, and the experiences of the many practitioners who respond to child online risk and safety problems through the Safer Internet Centre's Insafe Helpline assessment platform and case repository.

The wider context for this guide is the European Commission's new [strategy](#) (BIK+), adopted in 2022, to protect children from harmful and illegal online content and conduct, and promote their active participation in a digital world. By improving age-appropriate digital services, among other measures, the BIK+ initiative aims to empower children to make responsible choices and express themselves safely in the online environment.

The guide is organised as follows:

- An overview of the nature and prevalence of online risks encountered by children in Europe, classified according to [the 4Cs](#) of content, contact, conduct and contract risks.
- In depth examination of four case study risks: potentially harmful content online (a content risk); online sexual coercion and exploitation of children (a contact risk); online reputation (a conduct risk); and e-crime (a contract risk).
- Provision of a definition, information on prevalence and key issues, helpline case studies, and further resources for each case study risk.

## 2. What is online risk to children?

### i. Defining and classifying online risk to children

In a fast-changing digital ecosystem, the nature of risk is continually evolving, sometimes exposing children to emerging risks well before adults know how to mitigate them. No wonder that online risk is one of the most contested areas of children's digital experience, raising concerns for many stakeholders and posing pressing challenges for research, policy and practice.

Risk has been defined as the “*uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value*” (Aven & Renn, 2009, p. 1). This means that, for online risks encountered by children, we need to consider both the probability and severity of the harms that may result. By harm, we refer to a range of negative consequences to the child's emotional, physical or mental well-being. Whether or not online risk results in harm depends on a host of factors relating to the child, the actions of others, the technology, and the circumstances (Livingstone, 2013).

Online risk to children has been classified according to the 4Cs of content, contact, conduct and contract risks (Livingstone & Stoilova, 2021). The classification recognises that online risks arise when a child:

- Engages with and/or is exposed to potentially harmful CONTENT.
- Experiences and/or is targeted by potentially harmful CONTACT.
- Witnesses, participates in and/or is a victim of potentially harmful CONDUCT.
- Is party to and/or exploited by a potentially harmful CONTRACT.

 CORE	<b>Content</b>	<b>Contact</b>	<b>Conduct</b>	<b>Contract</b>
	Child engages with or is exposed to potentially harmful content	Child experiences or is targeted by potentially harmful <i>adult</i> contact	Child witnesses, participates in or is a victim of potentially harmful <i>peer</i> conduct	Child is party to or exploited by potentially harmful contract
<b>Aggressive</b>	Violent, gory, graphic, racist, hateful or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity, e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
<b>Sexual</b>	Pornography (harmful or illegal), sexualisation of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
<b>Values</b>	Mis/disinformation, age-inappropriate marketing or user-generated content	Ideological persuasion or manipulation, radicalisation and extremist recruitment	Potentially harmful user communities, e.g. self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
<b>Cross-cutting</b>	<b>Privacy violations</b> (interpersonal, institutional, commercial) <b>Physical and mental health risks</b> (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) <b>Inequalities and discrimination</b> (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

**Table 1: The 4Cs of online risks to children: the CO:RE classification** (Source: [Livingstone & Stoilova, 2021](#))

This classification was reviewed and updated by the European Commission-funded [CO:RE \(Child Online: Research and Evidence\) project](#) in consultation with the [Insafe network](#). The purpose was to ensure that the classification includes the many kinds of online risks of harm that children actually encounter. As a result of the consultation, more risks were added, including important crosscutting risks to children's privacy, health and fair treatment (see Table 1).

This classification was devised to assist stakeholders who work to minimise, mitigate or remedy online risks to children. Practitioners, such as the staff working in Insafe helplines, can use this in their and manage resources to mitigate risk.

## ii. Prevalence of online risk to children in Europe

Results from EU Kids Online's major survey of 25,101 European child internet users aged 9-16 years old (in 19 countries) indicated that children encounter a wide range of risks online ([Smahel et al., 2020](#)). Sexting and meeting new people on the internet were found to be the most common online risks. However, not all risks resulted in (self-reported) harm – 25 per cent of children reported being bothered or upset online in the past year.

Children do not report all the risks they encounter online to helplines, so the statistics of the cases that helplines deal with every year present a slightly different picture. Over the past year, the Insafe network of helplines across Europe<sup>1</sup> received a total of 56,891 queries related to online issues from children, parents, caregivers, teachers and social workers, among others. Of those, two-thirds (65 per cent) were made by children.

Since 2016 there has been an upward trend in the number of people contacting the helplines. For example, in the third quarter of 2016, there were just under 8,000 contacts, compared to 17,600 in the third quarter of 2022. Across countries, helplines can be reached by phone, online form, email, chat, SMS or other means.

Insafe records each contact received and categorises the reason for the contact against a predefined list of issues. The gender of the person making contact is also recorded along with the group that they represent (e.g. 5-11, 12-18, parent, teacher, social worker). There are helplines in all of the Member States, plus Iceland and Norway (see Annex II).

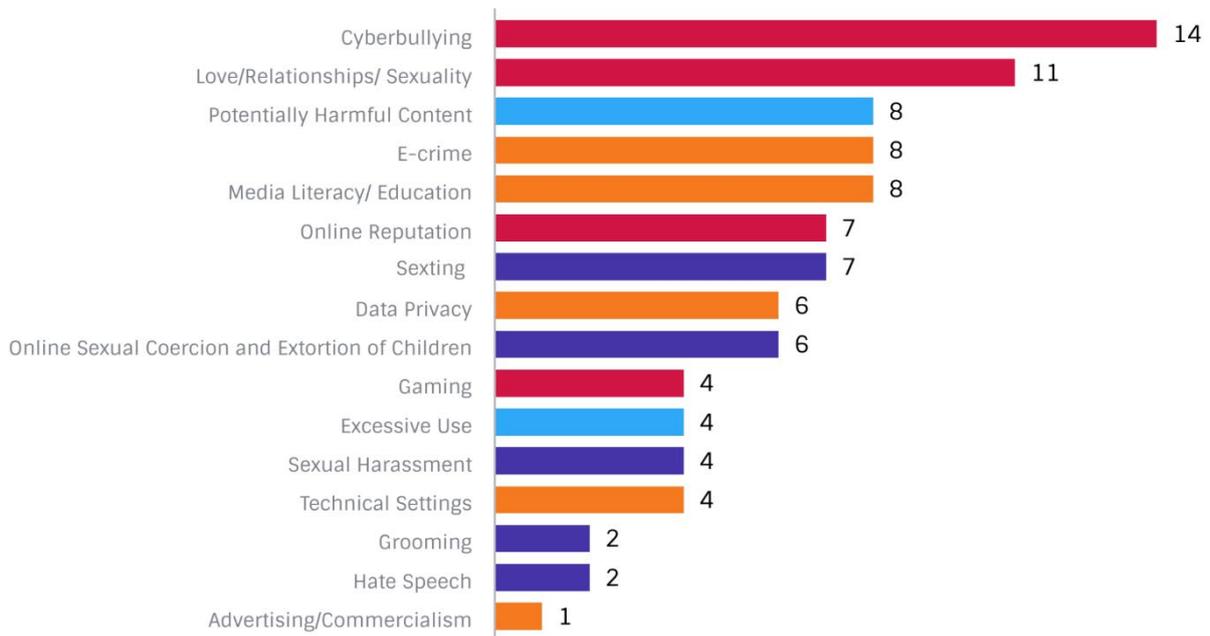
In the last two years, cyberbullying was the problem most frequently reported to helplines. Love, relationships and sexuality, as well as potentially harmful content, were the next most common categories reported. Recently, several helplines have noted increased contacts relating to e-crime.

Based on the risks reported to the helplines in 2022 (see Figure 1), we selected four risks to illustrate good practice responses to content, contact, conduct and contract risks: these are, respectively,

---

<sup>1</sup> Countries with Safer Internet Centre helplines include: Austria, Belgium, Croatia, Cyprus, Czech Republic (two helplines), Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland (two helplines); Italy; Latvia; Lithuania; Luxembourg; Malta; Netherlands; Norway; Poland; Portugal; Romania; Slovenia; Spain; Sweden; United Kingdom.

potentially harmful content, online sexual coercion and extortion of children, online reputation, and e-crime. Definitions of the helpline categories are provided in Annex I.<sup>2</sup>



**Figure 1: Percentage of contacts to European helplines, by online risk** (N= 56,891; Source: [BIK, 2022](#))

\* **Content** risks denoted in blue, **Contact** in purple, **Conduct** in red, and **Contract** in orange.

In the following sections, we map each risk onto the 4C matrix, and use case studies provided by the Insafe Coordination Team during 2022<sup>3</sup> to illustrate the problem reported and a helpline model response.

### 3. Content risk: potentially harmful online content

#### i. Definition

In an ideal world, children go online and engage with digital content that enables them to learn, create, enjoy and develop a [positive view](#) of themselves and respect for their and others' identity. While many opportunities arise from engaging with the digital environment, so too does the prospect of exposure to potentially harmful content. Age-inappropriate content ranges from violent, gory and graphic communication to hate speech, terrorism, online prostitution, drugs, eating disorders and self-harm ([Smahel et al., 2020](#)). This content may be generated by children or adults. While some online spaces are 'safe spaces', wherein the community of members provide support and deter individuals from harmful behaviour, they can also serve as a trigger or

<sup>2</sup> As of April 2023, Better Internet for Kids will update the categories and definitions to reflect the evolving online risk environment (see Annex I).

<sup>3</sup> We are grateful to colleagues across the Insafe helpline network who made these case studies available.

encouragement for unsafe action (Stoilova et al., 2021). Research shows that exposure to different types of harmful content is interrelated: so, if a child reports seeing one type of disturbing content, it is likely they have also seen other types.

The category of potentially harmful content online was added by the Insafe helpline network in 2013 and has been expanding as new topics are introduced. The most recent update distinguishes self-harm, suicide and hate speech as distinct categories (previously, they were grouped together).

## ii. Prevalence

Since 2020, exposure to potentially harmful content online has accounted for approximately 10 per cent of all calls received by helplines. Research on children's encounters with online risks across European countries (EU Kids Online, 2020) suggests that, on average, the most often reported harmful content was seeing hate messages (17 per cent), followed by gory or violent images (13 per cent), content suggesting ways to be thin (12 per cent), drug experiences (11 per cent), ways to physically harm themselves (10 per cent), and suicide methods (8 per cent). Thankfully, such exposure is not frequent, as the majority of children report that they have not seen harmful content online in the past year. However, there are substantial differences between countries (see Table 2).

	Ways of physically harming or hurting themselves	Suicidal ideation	Ways to be very thin	Hate messages that attack certain groups of individuals	Experiences of taking drugs	Gory or violent images	Sexual images online
<b>CH (Switzerland)</b>	9	5	8	13	14	10	17
<b>CZ (Czech Republic)</b>	18	10	17	25	15	17	26
<b>DE (Germany)</b>	2	2	3	4	3	6	**
<b>EE (Estonia)</b>	7	5	10	14	7	5	9
<b>*FI (Finland)</b>	18	8	10	17	10	11	**
<b>FR (France)</b>	7	4	9	8	6	7	4
<b>HR (Croatia)</b>	9	6	9	11	7	11	12
<b>IT (Italy)</b>	4	4	6	10	7	12	8
<b>MT (Malta)</b>	10	12	12	18	12	15	16
<b>NO (Norway)</b>	8	5	12	16	8	9	17
<b>PL (Poland)</b>	19	19	32	48	21	28	10
<b>PT (Portugal)</b>	10	9	12	17	13	15	16
<b>RO (Romania)</b>	8	12	12	18	13	18	13
<b>RS (Republic of Serbia)</b>	18	11	17	24	16	23	28
<b>*RU (Russian Federation)</b>	16	8	25	24	11	17	***
<b>SK (Slovak Republic)</b>	2	2	5	8	4	6	7
<b>*VL (Belgium)</b>	11	8	9	20	16	16	**
<b>Average</b>	10	8	12	17	11	13	14

**Table 2: Percentage of European internet-using children (12-16 years for all risks except 9-16 for sexual images) exposed to various types of harmful content (N = 25,101; Source: Smahel et al., 2020)**

\* FI/RU/VL: Data not weighted

\*\* Full age range not available

\*\*\* Question not asked

Q: "In the PAST YEAR, have you seen online content or online discussions where people talk about or ask any of these things?" (Percentage of children who answered "at least every month")

Below we expand on three of these types of harmful content.

### a. Hate messages

Hate messages are related to hate speech, which can be defined as:

*"All forms of communications that spread or promote discrimination, xenophobia and other forms of hatred based on intolerance"* ([Council of Europe, 2018](#)).

Hate messages attack certain groups or individuals based on race, religion, nationality, sexuality or other protected characteristics. Children can be exposed to hate messages that do not directly target them; or they can be the targets or perpetrators of hateful content. Between 4 per cent (Germany) and 48 per cent (Poland) of children in Europe reported seeing hate messages online in the previous year ([Smahel et al., 2020](#)). Older children are more likely to report seeing such messages than younger children, with this age difference especially pronounced in Poland and Malta.

### b. Eating disorders

This type of harmful content is related to problematic eating habits and eating disorders, such as anorexia or bulimia. Internet and social media are spheres where teenagers' everyday life takes place and they promote idealised and stereotyped beauty standards. Exposure to such imagery can lead to negative self-image and cause discontent and despondency ([Stoilova et al., 2021](#)). Findings from the [EU Kids Online Survey](#) indicate that, on average, 20 per cent of European children have seen online content or discussions on ways to be very thin. A gender difference is especially pronounced in the Czech Republic, Estonia, Finland, Norway and Poland ([Smahel et al., 2020](#)). [Pro-ana and pro-mia websites](#) can provide virtual spaces where teenagers exchange ideas about body image, and receive feedback on their physique and advice on how to lose weight.

### c. Ways to physically harm or hurt themselves

Self-harm can be defined as "non-suicidal self-injury" ([Kostyrka-Allchorne et al., 2022](#)), and is the act of harming oneself on purpose. Some examples are cutting oneself (for example, with a knife, razor blade or sharp object), burning oneself (with cigarettes, matches, candles), or punching, bruising or breaking one's bones. Self-harm is an unhealthy way to cope with emotional distress. While children who access such content tend to have existing mental health conditions, the online environment can contribute to exacerbating their problems ([Stoilova et al., 2021](#)). In the case of self-harm, online exposure to such content can be 'triggering', can allow the discovery of new methods of harm, or might normalise harmful behaviour.

The majority of children (64 per cent) surveyed by EU Kids online do not "frequently" encounter ways to physically harm or hurt themselves online. However, sporadic exposure (e.g. a few times per year) is more common, especially in the Czech Republic, Finland, Poland, Russia and Serbia ([Smahel, et al., 2020](#)).

### iii. Case studies

#### a. Malta

A school guidance teacher reached out for help in supporting a 9-year-old boy that she's supervising. The boy was initially reported by other children for exposing them to the Ouija spirit board through the school's individually assigned tablets. The teacher checked the device and found a lot of pornography links listed in the browser's history. This raised concerns both because the boy is very young, and because he managed to access such content on a school device, despite the filtering system in place. The teacher was worried about the type of content being viewed, whether it has been shared with other children in the school, and whether there are any safeguarding issues at the boy's home, for example, if he is being neglected. The teacher reached out to ask for the best way forward in addressing these concerns.

*The advice given was to reach out to the Department of Education which is responsible for the school's filtering system on these devices. The parent was already notified. The helpline offered to provide further support with any intervention, if needed, in particular to this child. The helpline also delivered an awareness-raising session with the whole class, by invitation from the school. The session covered a range of issues including age-appropriate content, peer pressure and the importance of speaking to a trusted adult if something has gone wrong. Specific support for the boy was also provided by the school.*

**Stop and think: Children can be curious about sexuality and seek information online especially if they do not feel that they can safely discuss these issues in person with trusted adults. Such curiosity might lead them to age-inappropriate material. It's best to have a preventative approach and use filters that block such material on devices that children use while also giving them an opportunity to learn about sex and sexuality in a supportive context, whether at home or school. It is important to remember that such material is not necessarily harmful to all children. Cultural specificity must also be taken into consideration, as an image might seem alarming in one context, but perhaps acceptable in another. Pornography provides a good entry point into discussions of age-appropriateness. The adult may want to find out how the child is feeling without making them feel guilty or ashamed, offer support if needed, explain why such material is not appropriate for their age, and find positive ways to address their curiosity. A more appropriate line of inquiry might be helping the child to determine what images are, or are not, illegal, abusive and exploitative.**

#### b. Greece

A mother called the helpline to ask for help concerning her 15-year-old daughter. After the pandemic, the girl had experienced difficulties creating and maintaining social relationships with peers. She started spending many hours online and became isolated from family members. The mother was really anxious about the online content her daughter was viewing as she had recently started mentioning metaphysics, spirits, sacrifices, Tarot cards, and so on. The mother asked for advice on how to spy on her daughter and check her mobile phone to find out if the girl was in danger.

*The counsellor provided active listening and support to the mother, highlighting the value of finding ways to help her daughter to start socialising with peers offline. The counsellor further explained that spying is not a good idea as it might encourage the girl to hide her activities and keep secrets from her parents. The counsellor advised the mother of ways to approach a supportive conversation with her daughter. They also suggested face-to-face family counselling sessions with a psychologist for further support, and recommended educational materials on adolescence and media literacy.*

**Stop and think: Spying on children can infringe their right to privacy, and their need for a space to explore and experiment without being monitored. It can also be counterproductive as it may encourage the child to hide their activities. Having a friendly conversation with the child about their interests and suggesting ways to make friends while staying safe online is a better approach.**

### c. Lithuania

A 14-year-old girl got in touch with the helpline to discuss her engagement with pro-anorexia and self-harm material. She had uploaded a full-body photo of herself (with clothes on), which was then shared in a pro-anorexia group. She shared that she felt good receiving likes and praise, and that she has never felt happier about her body. She wondered why aspiring to be very thin is seen as a bad thing. She also discussed self-harming, being proud of her scars, and watching suicidal ideation videos online.

*The counsellor validated the mixed feelings the caller expressed, including the curiosity and loneliness associated with eating disorders and self-harm experiences, but warned the girl about the dangers of engaging with potentially harmful content online. The caller was encouraged to continue speaking up about these topics, to seek support from trusted adults around her, and to consider professional help.*

**Stop and think: Glamorising eating disorders and self-harm on social media and the culture of “thinspiration” can normalise such behaviours and make some children unaware of the harms of such material. The algorithmic nature of the online environment can create “filter bubbles” meaning that young people may be bombarded with the same type of content, reinforcing their belief that this is normal.**

## iv. Resources

### Germany

This teaching unit "Challenges – All in good fun??" offers educational professionals suggestions on how to deal with the topic of 'social media challenges' and hoaxes with children and young people. An exercise to assess different challenges provides users with an opportunity to discuss the problematic aspects of such games:

<https://www.betterinternetforkids.eu/resources/resource?id=128657>

### Greece

This resource is addressed to parents, carers, and educators in order to advise them on how to talk to children about war and all the information they encounter about it online:

<https://www.betterinternetforkids.eu/resources/resource?id=129505>

### Italy

In this web series by the Italian Safer Internet Centre, each episode focuses on a different element of online safety, from strategies for handling cyberbullying to recognising and reporting unsafe/inappropriate interactions and content (e.g. zoombombing, body shaming, sexting, and so on):

<https://www.betterinternetforkids.eu/resources/resource?id=128766>

### Lithuania

In this video series, funny puppies are used to encourage the creation of a better internet by contacting the helpline:

<https://www.betterinternetforkids.eu/resources/resource?id=11327>

**Malta**

The members of the Maltese Youth Panel created a video to raise awareness of the impact of social media and influencers on body image. A corresponding lesson plan has been created for educators to use this video as a tool within the classroom:

<https://www.betterinternetforkids.eu/resources/resource?id=128649>

**Poland**

The Polish Safer Internet Centre created a mini-series of podcast recordings that address child online safety topics, such as cyberbullying, sexting, harmful content, and internet abuse:

<https://www.betterinternetforkids.eu/resources/resource?id=27118>

This campaign aims to prevent harmful beauty standards' impact on children and young people and support their body neutrality attitude:

<https://www.betterinternetforkids.eu/resources/resource?id=129496>

**Romania**

The Romanian Safer Internet Centre prepared a guide to harmful and illegal content online:

<https://www.betterinternetforkids.eu/resources/resource?id=128072>

**Slovenia**

This leaflet explains which online challenges are positive and which are negative, and which challenges we should tackle, but which we would be better off leaving out:

<https://www.betterinternetforkids.eu/resources/resource?id=129436>

## 4. Contact risk: Online sexual coercion and extortion of children

---

### i. Definition

Online sexual coercion and extortion of children is a form of digital blackmail where sexual information or images are used to extort sexual material, sexual favours or money. This category was previously classified as "sextortion" but replaced as the term was seen as less accurate.<sup>4</sup>

Online sexual coercion and extortion of children can have two aims:

- Sexual: including the procurement of sexual material (photos and/or videos) or a sexual encounter offline.
- Financial: gain financially when the victim pays money to prevent the sexual material from being shared more widely.

The Insafe helpline network introduced the category of "sextortion" at the beginning of 2018 following a marked rise in calls about this type of issue. The term "online sexual coercion and extortion of children" replaced "sextortion" in the classification from April 2023.

---

<sup>4</sup> The colloquial, often-used term "sextortion" is subject to debate in the field of child protection, as it does not show clearly that it is a matter of sexual exploitation against a child, therefore running the risk of trivialising a practice that can produce extremely serious consequences.

## ii. Prevalence

Sexual images, videos and messages always have the potential to be distributed and made public, outside of the sender's (and receiver's) control. Results from EU Kids Online indicate that sending sexual messages is less prevalent than receiving sexual messages. In most of the European countries surveyed, less than 10 per cent of children (aged 12-16) had sent sexual messages in the past year. Most children had also not received unwanted requests for sexual information; among those who had experienced unsolicited sexual messages and requests, it did not happen often (Smahel et al., 2020).

Since helplines began gathering data about online sexual coercion and extortion of children specifically, this problem has accounted for around 5 per cent of all calls that helplines receive. Discussions with industry have clarified that this is a growing problem often perpetrated by individuals who are located nowhere near the victim. In many cases, organised criminal gangs have been behind the threats; law enforcement agencies have discovered significant operations where people were working in shifts in order to try and blackmail as many individuals as possible to part with money or images.

Helplines have been made aware of cases where individuals were coerced into sharing images or doing sexual acts online believing that they were in a relationship with another person who had feelings for them. Originally occurring on sites such as [www.chatroulette.com](http://www.chatroulette.com) and [www.omegle.com](http://www.omegle.com), online sexual coercion and extortion of children has now moved to mainstream social media. Over the past two years, there were more cases of online sexual coercion and extortion of children that related to boys than girls reported to helplines.

The money transfers tend to be channelled through legitimate payment sites such as Western Union or via crypto currencies like Bitcoin. Several victims have paid large amounts of money in the hope that the videos and images would not be shared more widely. The amounts reported have varied between 50 to 15,000 Euros. Western Union has an [abuse help page](#) which provides links to useful information.

There are a number of scams associated with online sexual coercion and extortion of children as well. For example, one that has been circulating via email involves receiving an anonymous message telling the user that some malware has been installed onto their device allowing access to their browsing history and some very compromising video footage or images. The email usually contains the user password or one that they have used in the past, making them think that the claims about the webcam and videos and images are true. Reports have shown that these emails can be sent to tens of thousands of victims with the scammers only needing a fairly low hit rate to make money (BBC, 2019).

Advice from the police is that victims have done nothing wrong, they will be listened to and taken seriously.

## iii. Case studies

### a. Germany

A teenage boy called the helpline and explained that he met a really pretty girl online, they became friends and spent a lot of time online on a popular social networking site. They exchanged naked pictures. The girl then started threatening the boy saying that she wanted money or she would share the images. The boy was very frightened and said that he didn't have any money and

was worried about what would happen. He said he couldn't tell his parents as it was so embarrassing and needed help.

*The helpline response was to explain that this is not so unusual and that they had dealt with similar cases recently. They explained that the girl was breaking the law and told the boy not to pay any money. The counsellor advised the boy to save the evidence of the threats and requests for money, and to say that he was going to the police. It was also made clear that he should report and block her. Legal information was also shared, and the boy was advised to try and find some adult help and support from someone that he could trust.*

**Stop and think: Young people make new connections and friendships online. In most cases these are friends of friends but it is hard for young people to be certain about the identity of their online acquaintances. For example, the 'girl' may not be a girl after all; but if she is, she too may be in need of help and support.**

## b. Latvia

A 17-year-old boy was contacted by a girl on Instagram. They chatted for a few weeks and then decided to take their relationship to the next level by exchanging erotic photos. After this they decided to go even further, and the boy sent the girl a video of him masturbating in front of the camera. At this point the girl said that she was going to share the video with all of his friends on social media and his family and others that she had found on his Facebook page. She said that she would reconsider if he agreed to send more videos and also persuade someone else of his age to get involved and make videos together.

*The boy had a very strong sense of shame, betrayal, anger and helplessness, and it was important to help him towards a more stable state. He was given instructions not to share any more images and to block the girl and report her. He was also told to save all of the threatening messages as evidence of what had happened and to go to the police and explain what had happened. He was also advised to seek psychological support to help recover from the strong negative emotions he had experienced after the incident.*

**Stop and think: It is hard to say if the perpetrator was really a child as it was claimed. In cases where the perpetrator is a child, it is likely that they also need help and support. It is possible that they have also been a victim of sexual coercion and extortion.**

## c. Bulgaria

A 12-year-old girl contacted the helpline and explained that a fake Instagram profile had been blackmailing her. An unknown man had told her that if she didn't send nudes to him, he would contact her mother and say that she had been sending nudes to random people. The girl was very distressed by this and needed support.

*The counsellor advised the girl to report the case to the Safer Internet Centre's hotline and also to Instagram. She had already blocked the profile and wanted to know if the man might be able to photoshop her images and share them on social media. The counsellor acknowledged that this could happen but explained what to do and how to report this to the hotline. The girl was scared about telling her parents and the counsellor explained that she could get in touch again if she needed any additional support.*

**Stop and think: It might be difficult for children to distinguish real threats from fake ones, and make rushed decisions under pressure and end up in even more serious situations. It is important to encourage children to seek support early on to prevent problems from escalating.**

## iv. Resources

Helplines have had discussions about the issue and have suggested that the following advice could be helpful:

- Preserve and collect as much evidence as possible, including screenshots (showing the URL of the site being used).
- Block and remove the person who is blackmailing from all social media sites and platforms.
- Carry out a Google search to see if the image(s) are being share elsewhere.
- Set up a Google alert on your name so you will receive a notification if content is uploaded in the future.
- Check settings on social networks so that people who you don't know are unable to chat with you.
- Always report it if someone is targeting you in this way.

### Europol

A #SayNO guide for families and friends of victims of online sexual coercion and extortion of children (in Portuguese):

<https://www.betterinternetforkids.eu/resources/resource?id=22461>

<https://www.betterinternetforkids.eu/resources/resource?id=22458>

### France

A 'decision tree' for kids with useful tips and tricks to avoid becoming a victim of online sexual coercion and extortion of children:

<https://www.betterinternetforkids.eu/web/portal/resources/gallery?resourceId=12490>

### Latvia

Here are three short films by the Latvian Safer Internet Centre on different types of online sexual coercion and extortion of children:

*Derision* – <https://www.betterinternetforkids.eu/resources/resource?id=11191>

*Theft* – <https://www.betterinternetforkids.eu/resources/resource?id=11190>

*Rape* – <https://www.betterinternetforkids.eu/resources/resource?id=11189>

### Netherlands

A study on financial online sexual coercion and extortion of children in boys "Eigen Schuld, Dikke Bult":

<https://www.betterinternetforkids.eu/resources/resource?id=128787>

In this digital game, young kids solve puzzles to prevent the characters in the game from becoming victims (teachers can rent or buy the suitcase for their students):

<https://www.betterinternetforkids.eu/resources/resource?id=128039>

## 5. Conduct risk: online reputation

### i. Definition

Online reputation can be defined as the information that can be found about an individual online. It becomes a matter of concern when harm occurs as the result of the way that a child is perceived in the digital environment.

As with offline reputation, online reputation management encompasses the actions people take to monitor, analyse and shape the impressions they make on others. However, in the digital realm, online reputation encompasses the actions children have taken, such as items they have liked, shared and commented on, along with what others have shared about them. Even those individuals who have chosen not to sign up to one or more of the many social media platforms that are available today are not fully protected – they can still have an online reputation formed of content, data and information posted by others, or that they have inadvertently shared themselves through other sites.

Because children's online reputation can affect how people think or behave towards them, it is a topic worthy of critical attention. Online reputation tends to be important to young people who are generally quite careful and selective of what they share – and with whom – as a way of protecting their privacy online. Therefore, reputational damage can be quite upsetting for them.

### ii. Prevalence

According to the EU Kids Online survey, 7 per cent of children in Europe, ranging from 2 per cent in Croatia and 12 per cent in Romania, say that somebody used their personal information in a way that they did not like in the past year ([Smahel et al., 2020](#)). Four per cent of children said that somebody had created an online page or shared an image about them that was hostile or hurtful (ranging from 1 per cent in Croatia and 9 per cent in Romania ([Smahel et al., 2020](#))). Issues of family members sharing information about the child without their permission are more common. Between 8 per cent (Lithuania and Slovakia) and 36 per cent (Norway and Flanders) of children aged 12 to 16 years report that their parents/carers published information online without asking them (average of one in five children, 20 per cent). Nearly one in ten children (9 per cent) say that they were upset by this and an even higher proportion (14 per cent) report that they asked a parent to remove the content ([Smahel et al., 2020](#)).

The Insafe helpline network has been logging calls against the category 'online reputation' since 2013 under the heading "*concerns about damage to reputation online (this may include requests for information on how to protect online reputation)*". Calls to helplines regarding online reputation account for approximately 6-7 per cent of all calls across the EU.

There are three types of damage that can occur to the online reputation of children:

- When children share something that they will regret – such as an embarrassing photo or an offensive joke.
- When someone within the child's immediate familial circle posts information without the child's permission, such as 'sharenting'.
- When someone else shares something negative about the child.

Teaching young people to protect their reputation can have beneficial outcomes for later in life, for instance when education providers or employers might use their online information to make decisions about recruitment.

### iii. Case studies

#### a. Slovenia

A 12-year-old girl became friends with another girl on Instagram. Her new online acquaintance told her to take a video of herself in leggings. She did that and shared it with her new online acquaintance who promised not to publish the video but ended up posting it online. Now there are terrible comments under the video. She blocked the girl who posted the video and deleted their communication, but she was still very upset about what happened and called for help.

*The helpline took the time to listen to the girl calmly, giving her a feeling of security and acceptance. It was stressed that she was not to blame for the situation, as her new online acquaintance had broken her trust. The helpline advisor praised the girl for speaking up and advised her on how to report the video on Instagram, also referring her to an awareness centre where she can find information on how to protect her privacy. As the girl was receiving abusive comments online, the helpline further encouraged her to find someone to help her through this process – a competent adult in her environment. The advisor emphasised that it is okay to seek help and confidence at times like these, because each of us needs someone to lean on when we are having a hard time.*

**Stop and think: Children value their online reputation and can become really upset if damaging content is shared online, especially as such content can spread quickly. It is important that children know that they have the right to have such content removed, although this can be hard to achieve in practice. One useful strategy is to create positive content (e.g. set up a blog, leave nice comments on social media posts) so that the negative content will be pushed lower down on a profile or in the search results.**

#### b. Romania

A teenage girl contacted the helpline to explain that someone else had made an Instagram account using her name and data. The profile already had 11 posts with different photos of her. The girl wanted to know what could be done and was concerned that the photos and content could damage her reputation.

*The helpline explained about the reporting options that are available on Instagram and discussed some of the privacy settings in more detail. The counsellor talked about the importance of being in control of content and the difference between public and private settings.*

**Stop and think: The best strategy for this is preventative. A good tip to give to children is to regularly carry out a search using their name to see what content others are going to find if they do the same. They should use a few different search engines to see if there are differences. It is possible to**

**set up a Google alert<sup>5</sup> so that when content is shared publicly about them, they receive a notification about it.**

### c. Ireland

A teenage boy contacted the helpline and explained that someone was making false allegations about him on Snapchat. The allegations were serious, for example, that he had raped a girl. Apparently a lot of people believed the allegations and the boy was worried as his parents had initially believed them too. He was finding it very difficult to cope and was hurt that anyone would think it was okay to do this to him. He was finding it hard to sleep and had missed a lot of school as a result. He felt that everyone was talking about the situation, and he is still getting unpleasant messages on Snapchat.

*The counsellor listened to the caller and empathised with him. They then explored various options to deal with the situation. The caller proposed that he should close down his Snapchat account and also seek support from the school counsellor.*

**Stop and think: It is important to consider where the material damaging the child's reputation is hosted. The fastest way to resolve such an issue is to ask the person who posted it to remove it, but they might not agree. If the content breaks the terms and conditions on a site, then the site owner will remove it. It might be possible to have such content removed from search results using the 'Right to be forgotten legislation'<sup>6</sup>. This will not remove content from the web, only from the search results. [This is the form you need to complete.](#)**

## iv. Resources

### France

A resource developed to help children take a moment to reflect and think before publishing on the internet:

<https://www.betterinternetforkids.eu/resources/resource?id=8447>

### Greece

This guide informs readers on how to protect their online reputation:

[http://saferinternet4kids.gr/wp-content/uploads/2017/06/diadiptyakh\\_fhmh.pptx](http://saferinternet4kids.gr/wp-content/uploads/2017/06/diadiptyakh_fhmh.pptx)

### Luxembourg

Social media videos were produced to raise awareness around sexting, sharenting, self-presentation and online reputation:

<https://www.betterinternetforkids.eu/resources/resource?id=128636>

### Norway

As one part of a broader project on online privacy and surveillance-based advertising, "The Digital Tale" explores the way a digital trace can follow and affect lives:

<https://www.betterinternetforkids.eu/resources/resource?id=129446>

### Poland

"The Digital Footprint of a Little Child" is a publication that extols the dangers of carelessly posting

---

<sup>5</sup> <https://www.google.co.uk/alerts>

<sup>6</sup> <https://gdpr.eu/right-to-be-forgotten/>

about children, as well as good practices that will help parents of the youngest children skillfully manage their image:

<https://www.betterinternetforkids.eu/resources/resource?id=129552>

### Portugal

This awareness campaign poses the question “Are you real online?” to bring awareness to the possibilities and limits of using digital media in a playful and educational way:

<https://www.betterinternetforkids.eu/resources/resource?id=129456>

### Slovenia

This 14-question quiz assesses whether young people have the knowledge on how to manage their online reputation and that of others. Each question is also followed by a detailed explanation of the correct answer:

<https://www.betterinternetforkids.eu/resources/resource?id=129513>

### Sweden

Informed by a report produced by the Swedish Media Council and the Law and Internet Institute in Sweden, this resource highlights children's rights when carers publish information about their children on the internet, also referred to as 'sharenting':

<https://www.betterinternetforkids.eu/resources/resource?id=129515>

## 6. Contract risk: e-crime

### i. Definition

In an era of rapid technological advancement, children may become immersed in technology from an increasingly young age. In this guide, we have covered several of the current and emerging risks that accompany their journey online, but now turn to cybersecurity basics. While cyberattacks are not new, the extent to which children are targeted is less understood. E-crime is constantly evolving, but our current definition encompasses the following cyber threats:

- Identity theft – when a hacker steals someone's personal information and uses it for financial gain or other purposes.
- Fraud – using the internet to gain a dishonest advantage, often financial, over another person.
- Data theft – the illegal transfer or storage of personal, confidential, or financial information.
- Copyright infringement – when intellectual property is reproduced, distributed, performed or displayed without the permission of the owner.
- Hacking – the attempt to exploit a computer system to gain unauthorised access to personal or organisational data.
- Piracy – the online act of illegally copying or distributing of copyrighted material.

Children are an easy target for online fraudsters and hackers because they often have easy access to the internet, but only minimal knowledge of the risks.

## ii. Prevalence

Recent research indicates that a large proportion of young people (aged 16-19) in the EU are engaging in cybercrime, to such an extent that the conduct of low-level crimes online and online risk-taking is becoming normalised. Approximately half of the 8,000 respondents surveyed report engaging in a behaviour that could be considered a criminal offence in a jurisdiction (e.g. money muling, hate speech, hacking and fraud). In addition, 12 per cent use risky spaces which are intentionally hidden (such as Dark Web Forums), and 11 per cent use Darknet Markets which sell illegal goods.

The countries with the highest prevalence of respondents involved in cybercrime are Spain (75 per cent), Romania (73 per cent), the Netherlands (73 per cent) and Germany (72 per cent). A gender difference was also noted, with males being more likely to have been involved in cybercrime (74 per cent) compared to only 65 per cent of female respondents ([Davidson et al., 2022](#)).

Europe has been encountering several cyber threats, each creating a different set of problems and different set of solutions. The EU has been working to regulate cybercrime since 2001, when the first law on online fraud was passed. The 2013 Directive required all Member States to criminalise attacks against information systems, such as illegally accessing their materials or stealing an identity. The law mandates that cybercrime carry severe penalties, especially for cases of impersonation and fraud. However, this is still a relatively recent area of concern, and the legislative efforts to protect children from cybercrime and attacks are limited in a world of rapid, complex technological advancement.

The pandemic significantly increased the number of internet users and their activities online, and the methods used by fraudsters have improved. The number of calls to Insafe helplines regarding e-crime increased between the second and third quarter of 2022, with phishing being the leading type of online fraud in terms of losses. The scale of phishing has been growing significantly for the past few years, at more than 30 per cent annually.

## iii. Case studies

### a. Austria

The caller got in touch with the helpline because she recently came across a website via advertising on TikTok and ordered products (razors and accessories) online. Now she has received an open invoice from Klarna (a Swedish financial tech company that provides online financial services), but the website she ordered from has been deleted.

*The helpline advisor advised her not to pay the invoice until the problem is resolved and to contact Klarna support directly. If that doesn't help, he advises her to file a complaint to the Internet Ombudsstelle.*

**Stop and think: Financial fraud can be really difficult for children to identify. It is important to encourage children to consult an adult before making purchases from unknown sellers and to think about the long-term consequences which might include the theft of their financial details.**

### b. Spain

A call was received from a 17-year-old boy who was worried about his Instagram account being hacked. He explained that he had become the victim of identity theft and was no longer able to access his Instagram account as the password and email associated with the account seemed to

have been changed. He did not know how the identity theft happened or who could have stolen his credentials. He could see that his account was being misused – fake Bitcoins were published from his stolen account, as well as suspicious adverts for cryptocurrencies with potentially malicious links. Some of his friends told him that they were contacted from his account with suspicious offers. When he called INCIBE's *Your Help in Cybersecurity* service he had already reported what had happened on social media. The boy wanted to know what else he could do.

He was given guidelines for both online fraud and device protection, including:

- Keep antivirus software updated on your phone and run it to see if the phone is infected.
- Once you have cleaned your device, update all passwords with new more robust ones.
- Tell your contacts what has happened so they can avoid falling for the same fraud too.
- Keep all the evidence you can (screenshots, saved messages, and so on). This will help you if you wish to report the crime.
- To check if your personal details have been stolen and are being fraudulently used, you can carry out 'ego-surfing' (i.e. searching for your own name online in order to review the results).
- Do not access shortened or suspicious URLs. Use URL analysis tools to detect viruses, worms, trojans and all types of malware.
- Use two-factor authentication.
- A possible next step would be to report to the Spanish Data Protection Agency (AEPD) and the police and to send an email to [incidencias@cert-incibe.es](mailto:incidencias@cert-incibe.es) to report the fraudulent URL.

**Stop and think: Children use their social media to stay in touch with friends and not being able to access their accounts can be troublesome and upsetting. Information posted from their accounts can also damage their relationships with peers and can affect their online reputation, so supporting children to manage these situations is important.**

### c. Luxembourg

A mother called because her 12-year-old son's Google account and his gaming account had been hacked. All data and content (videos) had been changed and it was not possible to regain access to the accounts. The gaming account had already been sold. The family had contacted the game company, but they claimed they could not do anything because the boy could not prove that he was the owner of the account.

The helpline advised the mother to take the following practical actions (with relevant contacts provided): (i) check that there is no malware on the computer, (ii) using a different device, try to regain access to the affected accounts (hopefully with the support of the gaming company); (iii) secure the account by closing any open sessions and changing the password to a strong password combined with two-factor authentication; (iv) block credit cards that may have been compromised); (v) consider filing a complaint with the police (or National Data Protection Commission) if the damage was considerable. They also suggested ways for the mother to support her son in dealing with his frustration and anger. This included discussing how she can prepare her son for the fact that maybe the account cannot be restored, meaning his efforts were in vain and he has to build up the world of play again.

**Stop and think: It can take a lot of effort and careful curation to create one's online presence and gain a stable base of followers. Therefore, it can be upsetting for children to have their hard work stolen.**

## iv. Resources

### Czech Republic

A short video about internet security was both scripted and filmed by students from the Czech Youth Panel:

<https://www.betterinternetforkids.eu/resources/resource?id=128668>

### Greece

Through an imaginative video created with humour, the Greek Safer Internet Centre aims to educate citizens in cyber first aid and protect users from various forms of online fraud:

<https://www.betterinternetforkids.eu/resources/resource?id=129506>

An informative video on how to protect users from phishing and smishing:

<https://www.betterinternetforkids.eu/resources/resource?id=128703>

### Lithuania

The flyer introduces examples of phishing that occur through various apps and e-services, social engineering, and offers advice to recognise phishing and avoid losses:

<https://www.betterinternetforkids.eu/resources/resource?id=129614>

## 7. Conclusion

New online technologies are increasingly embedded in children's lives. As such, there are emerging questions about their social implications and consequences. While today's youth are often at the forefront of media adoption, they are also prone to a range of ever-evolving, risky or negative experiences for which they may not be fully prepared.

This good practice guide has focused on the nature and prevalence of select online risks encountered by children across European countries. It is important to bear in mind that not all children experience risk to the same degree. As the results from the EU Kids Online network indicate, socio-demographic factors (such as age, gender and nationality) make a difference when it comes to encountering risks.

Understanding risk requires an acknowledgement that what is defined as a risk to one child might be an opportunity for another. For instance, sexting can begin as positive and exciting, but as illustrated by the section on online sexual coercion and extortion, can also lead to distress and potential harm. In the case studies presented here, we focused on the negative experiences, specifically, and have highlighted good practices by which professionals can respond constructively.

Moreover, the categories and definitions are also subject to continual change. In Annex I, you will find the newly approved BIK classification of online risks. While there is scope to debate the definitions and categorisation, the evidence presented in this guide documents that the internet affords significant risk of harm to children, and this requires societal efforts to mitigate and remedy.

The question of which strategies work best is difficult to answer. While there is no easy one-size-fits all solution, the aim of this good practice guide has been to increase awareness of the myriad online risks of harm to children and to encourage the use of tools and services available, as illustrated by case studies of positive help and support. The resources presented here are a starting point.

Across Europe, Safer Internet Centre helplines offer advice and support to young people on how to deal with harmful online content, contact, conduct and contracts (see Annex II). Dedicated call centres can be accessed by children, and can work in collaboration with parents, caregivers, schools and communities to equip children with the skills to not only confront digital risks, but also maximise online opportunities.

## Bibliography

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, 12(1), 1–11. <https://doi.org/10.1080/13669870802488883>

Better Internet for Kids. (2020). Positive online content for children: Best practice guide. [https://www.betterinternetforkids.eu/documents/167024/3974002/POCC\\_BestPracticeGuide.pdf/7606c4a8-e6ac-4980-a6ab-1c2099597948](https://www.betterinternetforkids.eu/documents/167024/3974002/POCC_BestPracticeGuide.pdf/7606c4a8-e6ac-4980-a6ab-1c2099597948)

Better Internet for Kids. (2022). Quarterly bulletin. <https://www.betterinternetforkids.eu/practice/bik-bulletin>

Council of Europe. (2018). Hate speech. <http://www.coe.int/en/web/freedom-expression/hate-speech>

Davidson, J., Aiken, M.P., Phillips, K., & Farr, R.R. (2022). European youth cybercrime, online harm, and online risk taking: 2022 research report. Doi: [10.13140/RG.2.2.20477.03049/1](https://doi.org/10.13140/RG.2.2.20477.03049/1)

Kostyrka-Allchorne, K., Stoilova, M., Bourgaize, J., Rahali, M., Livingstone, S., & Sonuga-Barke, E. (2022). Review: Digital experiences and their impact on the lives of adolescents with pre-existing anxiety, depression, eating and non-suicidal self-injury conditions. *Journal of Child and Adolescent Mental Health*. <https://pubmed.ncbi.nlm.nih.gov/36478091/>

Livingstone, S. (2013). Online risk, harm and vulnerability: reflections on the evidence base for child Internet safety policy. *Journal of Communications studies*, 18(35), 13-28. <http://eprints.lse.ac.uk/62278/>

Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children*. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE – Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.71817>

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. <https://doi.org/10.21953/lse.47fdeqj01of0>

Smahel, D., Machackova, H., Smahelova, M., Cevelicsek, M., Almenara, C.A., & Holubciová, J. (2018). *Digital technology, eating behaviors, and eating disorders*. Springer.

Stoilova, M. (2021). What to be mindful of: children's mental health and the digital environment. *Parenting for a Digital Future*. 06 Oct 2021. [http://eprints.lse.ac.uk/112874/1/parenting4digitalfuture\\_2021\\_10\\_06\\_childrens\\_mental.pdf](http://eprints.lse.ac.uk/112874/1/parenting4digitalfuture_2021_10_06_childrens_mental.pdf)

Stoilova, M., Edwards, C., Kostyrka-Allchorne, K., Livingstone, S., & Sonuga-Barke, E. (2021). Adolescents' mental health vulnerabilities and the experience and impact of digital technologies. London School of Economics and Political Science and King's College London. [http://eprints.lse.ac.uk/112931/3/Stoilova\\_et\\_al\\_2021\\_Mental\\_health\\_digital\\_technologies\\_report.pdf](http://eprints.lse.ac.uk/112931/3/Stoilova_et_al_2021_Mental_health_digital_technologies_report.pdf)

## Annex I: Category definitions (BIK, 2023)

The updated list of categories and definitions below is coming into force from April 2023.

Category	Definition
<b>Advertising/commercialism</b>	Misleading policies, terms and conditions, fake advertising.
<b>Data privacy</b>	Issues related to the abuse of personal or private information, as well as how to protect privacy and how to react when something has gone wrong.
<b>Fake news</b>	False or misleading information which is presented as factual – either unintentionally (misinformation) or intentionally (disinformation).
<b>Media literacy education</b>	Callers asking for information relating to a better understanding of the internet, online services and how they can be used.
<b>Potentially harmful content</b>	Including online prostitution, drugs, eating disorders, etc. Any issues not covered by other categories.
<b>Self-harm</b>	The non-suicidal injuring of one's body.
<b>Suicide</b>	Including calls related to sites promoting suicide and explaining ways to commit suicide.
<b>Technical settings</b>	Where a caller needs help to alter settings – filtering and parental controls, anti-virus, spam, etc.  Including security maintenance (for a device) (e.g. firewall, updates, popups, cookies).
<b>Hate speech</b>	Discrimination or prejudice against others on account of their race, religion, ethnic origin, sexual orientation, disability or gender – this could include racist materials online or racist comments which have been made by a group or individual.
<b>Cyberbullying</b>	Bullying usually involves a child being picked on, ridiculed and intimidated by another child, other children or adults using online technologies.  Bullying may involve psychological violence.

	Cyberbullying can be intentional and unintentional.
<b>e-crime</b>	Chain emails, phishing sites, identity theft, fraud, data theft, copyright infringement, hacking, piracy, etc. This may include referrals to a hotline.
<b>Radicalisation/terrorism</b>	The unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims. This includes grooming for violent extremism.
<b>Excessive use</b>	Calls related to the amount of time spent on media – related to the loss of control over internet or online use as compared to other (offline) activities.
<b>Gaming</b>	For any issues related to gaming content (e.g. pay to win, loot boxes). Please note that addiction should be logged under excessive use.
<b>Love/relationships/sexuality (online)</b>	Questions relating to online love, relationships, dating sites etc. This category includes consensual sexting.
<b>Online reputation</b>	Concerns about damage to reputation online (this may include requests for information on how to protect online reputation).
<b>Pornography</b>	Online content with no artistic value that describes or shows sexual acts or naked people in a way that is intended to be sexually exciting.
<b>Grooming</b>	Actions deliberately undertaken (sometimes, but not always over a longer period of time) by an adult or stranger with the aim of befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual activity with the child.
<b>NCSII</b>	The non-consensual sending or receiving of sexual images and/or texts via mobile and other devices (including appearing in such images) among peers. This includes cyberflashing. Consensual sexting should be recorded under the category love/relationships/sexuality (online).
<b>Online sexual coercion and extortion of children (formerly referred to as sextortion)</b>	A means of coercing cybercrime victims to perform sexual favours or to pay a hefty sum in exchange for the non-exposure of their explicit images, videos or conversations.

## Annex II: Safer Internet Centre services and resources, by EU country<sup>7</sup>

	Awareness centre website	Helpline website
Austria	<a href="https://www.saferinternet.at">https://www.saferinternet.at</a>	<a href="https://www.rataufdraht.at">https://www.rataufdraht.at</a>
Belgium	<a href="http://www.clicksafe.be">http://www.clicksafe.be</a>	<a href="http://www.clicksafe.be">http://www.clicksafe.be</a>
Bulgaria	<a href="http://www.safenet.bg">http://www.safenet.bg</a>	<a href="https://www.safenet.bg">https://www.safenet.bg</a>
Croatia	<a href="http://www.csi.hr">http://www.csi.hr</a>	<a href="https://csi.hr/helpline">https://csi.hr/helpline</a>
Cyprus	<a href="https://www.cybersafety.cy">https://www.cybersafety.cy</a>	<a href="https://www.cybersafety.cy/helpline">https://www.cybersafety.cy/helpline</a>
Czech Republic	<a href="https://www.bezpecnenanetu.cz">https://www.bezpecnenanetu.cz</a>	<a href="http://www.linkabezpeci.cz">http://www.linkabezpeci.cz</a> and <a href="https://www.ditekrize.cz">https://www.ditekrize.cz</a>
Denmark	<a href="https://sikkertinternet.dk">https://sikkertinternet.dk</a>	<a href="http://www.cfdp.dk">http://www.cfdp.dk</a>
Estonia	<a href="https://www.targaltinternetis.ee">https://www.targaltinternetis.ee</a>	<a href="https://www.lasteabi.ee">https://www.lasteabi.ee</a>
Finland	<a href="https://www.saferinternet.fi">https://www.saferinternet.fi</a>	<a href="https://www.mll.fi/nuortennetti">https://www.mll.fi/nuortennetti</a>
France	<a href="http://www.saferinternet.fr">http://www.saferinternet.fr</a>	<a href="http://www.3018.fr">http://www.3018.fr</a>
Germany	<a href="http://www.saferinternet.de">http://www.saferinternet.de</a>	<a href="https://www.nummergegenkummer.de">https://www.nummergegenkummer.de</a>
Greece	<a href="http://saferinternet4kids.gr">http://saferinternet4kids.gr</a>	<a href="http://www.help-line.gr">http://www.help-line.gr</a>
Hungary	<a href="http://saferinternet.hu">http://saferinternet.hu</a>	<a href="https://www.kek-vonal.hu">https://www.kek-vonal.hu</a>
Iceland	<a href="http://www.saft.is">http://www.saft.is</a>	<a href="http://www.raudikrossinn.is/page/rki_hv_ad_hjalparsiminn">http://www.raudikrossinn.is/page/rki_hv_ad_hjalparsiminn</a>
Ireland	<a href="https://www.webwise.ie">https://www.webwise.ie</a>	<a href="http://www.childline.ie">http://www.childline.ie</a> and <a href="http://www.npc.ie">http://www.npc.ie</a>
Italy	<a href="http://www.generazioniconnesse.it">http://www.generazioniconnesse.it</a>	<a href="http://www.azzurro.it/it/cosa-facciamo/pronti-allascolto/pronto-telefono-azzurro">http://www.azzurro.it/it/cosa-facciamo/pronti-allascolto/pronto-telefono-azzurro</a>
Latvia	<a href="https://www.drossinternets.lv">https://www.drossinternets.lv</a>	<a href="http://www.bti.gov.lv">http://www.bti.gov.lv</a>
Lithuania	<a href="https://www.draugiskasinternetas.lt">https://www.draugiskasinternetas.lt</a>	<a href="http://www.vaikuliniija.lt">http://www.vaikuliniija.lt</a>
Luxembourg	<a href="https://www.bee-secure.lu">https://www.bee-secure.lu</a>	<a href="https://www.bee-secure.lu/helpline">https://www.bee-secure.lu/helpline</a>
Malta	<a href="http://www.besmartonline.org.mt">http://www.besmartonline.org.mt</a>	<a href="https://fsws.gov.mt/en/appogg/Pages/welcome-appogg.aspx">https://fsws.gov.mt/en/appogg/Pages/welcome-appogg.aspx</a>

<sup>7</sup> List is correct as of February 2023.

The Netherlands	<a href="https://saferinternetcentre.nl">https://saferinternetcentre.nl</a>	<a href="https://www.meldknop.nl">https://www.meldknop.nl</a>
Norway	<a href="https://www.medietilsynet.no/om-medietilsynet/pagaende-prosjekter-og-utredninger/norges-safer-internet-center">https://www.medietilsynet.no/om-medietilsynet/pagaende-prosjekter-og-utredninger/norges-safer-internet-center</a>	<a href="http://www.korspahalsen.no">http://www.korspahalsen.no</a>
Poland	<a href="http://www.saferinternet.pl">http://www.saferinternet.pl</a>	<a href="http://www.116111.pl">http://www.116111.pl</a>
Portugal	<a href="http://www.internetsegura.pt">http://www.internetsegura.pt</a>	<a href="http://www.internetsegura.pt/linha-ajuda">http://www.internetsegura.pt/linha-ajuda</a>
Romania	<a href="http://www.oradenet.ro">http://www.oradenet.ro</a>	<a href="https://oradenet.salvaticopiii.ro/ctrl-ajutor">https://oradenet.salvaticopiii.ro/ctrl-ajutor</a>
Slovenia	<a href="http://www.safe.si">http://www.safe.si</a>	<a href="http://www.e-tom.si">http://www.e-tom.si</a>
Spain	<a href="https://www.is4k.es">https://www.is4k.es</a>	<a href="https://is4k.es/ayuda">https://is4k.es/ayuda</a>
Sweden	<a href="https://www.statensmedierad.se/om-statens-medierad/safer-internet-centre">https://www.statensmedierad.se/om-statens-medierad/safer-internet-centre</a>	<a href="https://www.bris.se">https://www.bris.se</a>