At its 40th meeting on 15-16 November 2016, the Working Party on Security and Privacy in the Digital Economy (SPDE) discussed the process for the review of the 2012 Recommendation on the Protection of Children Online and agreed, as a first step, to circulate a questionnaire to delegations on the implementation and continued relevance of the Recommendation. This paper includes information on the questionnaire and timelines for responses.

Developed in consultation with the SPDE Bureau, the subsequent questionnaire is now available online. Delegates will receive the link to the questionnaire by email and are asked to submit their answers by March 31, 2017. The use of a hard copy version of the questionnaire is possible, but will generate additional work for the Secretariat as responses will have to be transferred into the standard electronic format. Hard copies should be sent by the same date to: Elettra.ronchi@oecd.org and Claire.Hilton@oecd.org.

Main contacts: Elettra Ronchi: Elettra.Ronchi@oecd.org; Claire Hilton: Claire.Hilton@oecd.org
NOTE BY THE SECRETARIAT

The Recommendation on the Protection of Children Online was adopted by the OECD Council on 16 February 2012. It instructs the CDEP to review this Recommendation and its implementation and to report to Council within five years of its adoption and thereafter as appropriate.

At its 40th meeting on 15-16 November 2016, the Working Party on Security and Privacy in the Digital Economy (SPDE) discussed the process for the review and agreed, as a first step, to circulate a questionnaire to delegations on the implementation and continued relevance of the Recommendation. On the basis of responses to the questionnaire a short report will be prepared and circulated. Delegates at the SPDE meeting in May 2017 will be invited to discuss the report and agree on the way forward for the review.

Developed in consultation with the SPDE Bureau, the subsequent questionnaire is now available online. Delegates will receive the link to the questionnaire by email and are asked to submit their answers by March 31, 2017. The use of a hard copy version of the questionnaire is possible, but will generate additional work for the Secretariat as responses will have to be transferred into the standard electronic format. Hard copies should be sent by the same date to: Elettra.Ronchi@oecd.org and Claire.Hilton@oecd.org.

---


OBJECTIVE OF THE REVIEW AND QUESTIONNAIRE

1. The questionnaire annexed to this document - developed in consultation with the Bureau of the Working Party on Security and Privacy in the Digital Economy (SPDE) - aims to support the first review of the 2012 OECD Council Recommendation on the Protection of Children Online (Recommendation), as called for in its final provision.

2. The purpose of the review is to ensure that the Recommendation is still relevant to guide policy development and will continue to be so for at least for the next five years. In particular, the review process provides an opportunity to:
   - Establish whether and how the Recommendation has been implemented in member countries, and review developments since 2012 in children online protection policy;
   - Identify areas where the Recommendation may need to be updated, as appropriate;
   - Assess the potential impact of contextual changes (e.g. technologies, usage, threats, etc.) and on the continued relevance of the Recommendation.

3. On the basis of the responses to the questionnaire, an analytical report will be developed to support a discussion by OECD delegations on the continued relevance of the Recommendation and the need to revise it. It will provide directions and options for possible improvement of the Recommendation, as appropriate, to be discussed at the meeting of the SPDE on May 15-16, 2017.

ORIGINAL SCOPE OF THE RECOMMENDATION

4. The Recommendation on the Protection of Children Online was adopted by the OECD Council on 16 February 2012. It instructs the CDEP to review this Recommendation and its implementation and to report to Council within five years of its adoption and thereafter as appropriate.

5. The Recommendation focuses on the protection of children as users of the Internet. It encompasses content risks, contact risks, risks related to children as consumers as well as information security and privacy risks faced by children on the Internet (Figure 1).

---

Figure 1. Typology of risks used for the development of the Recommendation

6. The Recommendation does not address child pornography or the sexual exploitation of children on the Internet. This separate treatment was deemed justified because it calls for radically different measures to protect children and in some cases may require law enforcement cooperation such as through Interpol. At the same time, as noted in paper DSTI/CDEP/SPDE(2016)2, texting and the social sharing of short videos and live broadcasting (for example on twitter, instagram, snapchat etc) have become a centerpiece in teen social life, and parents, educators and advocates have grown increasingly concerned about the potential misuse of mobile phones in the sexual interactions of teens and young adults.

Structure of the Recommendation

7. The Recommendation, which is reproduced in Annex I, is organised in 3 sections. The first section covers Policy making for all stakeholders. It calls for:

- Empowering children, recognising the primary role of parents in minimising risks to their children online (as they do offline).

- The adoption of policy measures proportionate to the risks, respecting fundamental values, and seeks to avoid undermining the framework conditions that have enabled the Internet to succeed.

- Flexibility to address differing ages and vulnerabilities among children.

8. The second main section covers Domestic policy making by governments and recognises that good policy making requires leadership, co-ordination, coherence, awareness raising, evidence, and technology solutions.

9. The final section addresses International policy making by governments and addresses the importance of international networks, information and data sharing, capacity building, and the participation of other intergovernmental organisations.
Questionnaire format

10. The questionnaire (Annex II) is subdivided into seven short sections:

- Implementation and enforcement
- Leadership and responsibility
- Monitoring and evaluation of policies
- Measuring online risks for children
- Review of the 2012 Recommendation
- Other
- Relevant technological developments

11. It is circulated to SPDE member and non-member country delegations online. Responses should reflect their government’s view regarding the policy framework for the protection of children online.

12. Other delegations, such as from business and industry (BIAC), civil society (CSISAC) and the Internet technical community (ITAC) are invited to provide a position paper on the review of the 2012 Recommendation instead of responding to the questionnaire which is primarily designed to collect information from governments.

13. All responses will be shared on the SPDE delegates’ workspace at: https://community.oecd.org/community/children-comm/wpisp.

How to respond

14. Developed in consultation with the SPDE Bureau, the subsequent questionnaire is now available online. Delegates will receive the link to the questionnaire by email and are asked to submit their answers by March 31, 2017. They are asked to provide as much information, descriptions and references as possible in response to the questions in order to enable a substantive assessment of how the Recommendation is being implemented in their country, and whether and how the Recommendation could be improved.

15. The use of a hard copy version of the questionnaire is possible, but it will generate additional work for the Secretariat as responses will have to be transferred into the standard electronic format. Hard copies should be sent by the same date, March 31 2017 to: Elettra.ronchi@oecd.org and Claire.Hilton@oecd.org.
Overview of Timelines

- Responses to the questionnaire should be received by **March 31, 2017**.
- BIAC, CSISAC and ITAC are invited to provide their position paper on the review by **the same date**.
- The draft report will be circulated in April 2017 for discussion at the May 2017 SPDE meeting where delegates will be invited to agree on next steps, including on whether to revise the Recommendation.
ANNEX I

DRAFT RECOMMENDATION OF THE COUNCIL ON
THE PROTECTION OF CHILDREN ONLINE

THE COUNCIL,

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;


RECOGNISING that a growing number of children are spending increasing time online, starting at younger ages, and that Internet technologies and access devices are evolving rapidly, facilitating the access of children to the Internet and changing their online usage patterns;

RECOGNISING that while the Internet brings major benefits to children in terms of education, self-expression, and social development, its use also carries a spectrum of risks to which children are more vulnerable than adults;

RECOGNISING the importance of co-operation and information sharing by all stakeholders in the development, implementation and assessment of policy approaches to the protection of children online;

RECOGNISING that the protection of children online requires policies which both reduce online threats to foster a safer Internet for children and enable children to protect themselves from threats that remain;

RECOGNISING that even if regional and local cultural differences impact the evaluation of online risks to children, international dialogue and co-operation has proven valuable to establish more effective policy approaches for an inherently global medium like the Internet:

On the proposal of the Committee for Information, Computer and Communications Policy:

1. AGREES that, for the purpose of this Recommendation:

   i) “Children” encompass every human being below the age of eighteen years, recognising that a lower age threshold might be appropriate in providing certain legal protections; “parents” encompass children’s parents and carers;
ii) The “protection of children online” encompasses content risks, contact risks, risks related to children as consumers as well as information security and privacy risks faced by children on the Internet;

iii) “Stakeholders” encompass governments, businesses, civil society and the Internet community and other entities involved in maintaining a safe Internet and educating children.

2. AGREES that this Recommendation does not cover risks related to child sexual abuse images online and the sexual exploitation of children which are matters addressed by other international instruments;

3. RECOMMENDS that in formulating policies for the protection of children online, governments and all other stakeholders take into account the following principles:

1. a. Empowerment

   i) Policies to protect children online should recognise that all stakeholders share responsibility both to make a safer online environment for children by reducing online threats to children, and to support the primary role of parents in evaluating and minimising risks of harm to their children online as well as offline;

   ii) Policies to protect children online should empower children and parents to evaluate and minimise risks and engage online in a secure, safe and responsible manner.

2. b. Proportionality and fundamental values

   i) Policies to protect children online should be proportionate to the risks, effective and balanced. They should maximise the protection against online risks faced by children without restricting the opportunities and benefits of the Internet for children as well as for other users.

   ii) Policies to protect children online should not undermine the framework conditions that enable the Internet to operate as a global open platform for communication, innovation, economic growth, and social progress. The consistency of policies designed to protect children online with other economic and social Internet policies should be carefully assessed prior to adoption and implementation.

   iii) Policies to protect children online should be consistent with fundamental values of democratic societies as they apply to all individuals including children. In particular, they should support freedom of expression, privacy protection and the free flow of information.

3. c. Flexibility

   i) Policies to protect children online should be age-appropriate and accommodate developmental differences and special vulnerabilities. Where age-based restrictions are established, all stakeholders should strive to ensure that such restrictions are respected.

   ii) Policies to protect children online should be technology neutral to ensure their sustainability in a dynamic environment characterised by rapidly evolving technologies and patterns of usage.

4. RECOMMENDS that, in formulating policies at the domestic level for the protection of children online, governments:
a. Demonstrate leadership and commitment to protect children online by:

   i) Adopting clear policy objectives at the highest level of government;

   ii) Identifying government bodies with responsibility and authority to implement these policy objectives and to co-operate across borders;

   iii) Developing policies that are inclusive of all stakeholders and rely on a mix of public and private, voluntary and legal, awareness raising, educational and technical measures to protect children online.

b. Support a co-ordinated response from all stakeholders by facilitating and, as appropriate, establishing:

   i) An open dialogue in order to foster synergies, benefit from the expertise of all stakeholders including parents, educators and the children themselves and take into account their perspectives;

   ii) Partnerships to develop self- and co-regulatory programmes characterised by transparency and accountability.

c. Foster consistency and coherence of domestic child online protection initiatives across public and private stakeholders. This could include:

   i) Ensuring the enforcement of existing protection measures;

   ii) Clarifying the categories of risks and harmonising the terminology used to inform the public;

   iii) Promoting mutually reinforcing policy measures rather than accumulating isolated or stand-alone, and potentially inconsistent, initiatives.

d. Foster awareness raising and education as essential tools for empowering parents and children by, for example:

   i) Integrating Internet literacy and skills in school curricula with a focus on risks and appropriate online behaviour;

   ii) Training educators and encouraging other stakeholders to educate and raise awareness of children and parents;

   iii) Regularly measuring the evolution of their Internet literacy.

e. Support evidence-based policies for the protection of children online by:

   i) Facilitating the further development of a robust empirical and analytical basis, including undertaking longitudinal surveys, with a view to support policy development and implementation through better understanding Internet usage by children, risk evolution and awareness;
ii) Conducting regular impact assessments of policies, including of co- and self-regulatory initiatives.

f. Encourage the development and adoption of technologies for the protection of children online that respect the rights of children and the freedom of other Internet users. This could include:

i) Fostering further research on privacy protective, interoperable and user friendly technical measures, including parental controls and age verification systems;

ii) Promoting the use of technologies which enable children to protect themselves against online risks;

iii) Fostering the assessment of the potential impact of such technical measures in relation to fundamental values such as freedom of expression, privacy protection and the free flow of information, as well as the implementation of appropriate safeguards;

iv) Promoting labelling schemes attesting the trustworthiness, quality and user friendliness of such technical measures.

5. **RECOMMENDS** that, at the international level, governments:

a. Strengthen international networks of national organisations dedicated to the protection of children online such as networks of hotlines and awareness centres and, where appropriate, facilitate an expansion of their role.

b. Share information about national policy approaches to protect children online and in particular develop the empirical foundations for quantitative and qualitative international comparative policy analysis. This could include:

i) The adoption of a shared statistical framework enabling international comparability of indicators on children use of the Internet, risk prevalence, awareness by children and parents of these risks and of how to respond to them, as well as policy impact and efficiency;

ii) The harmonisation of the statistical definition of risks and related policy responses as well as children’s age groups used for statistical purposes;

iii) A shared commitment to regularly update official quantitative data within a timeframe that takes into account the dynamic development of the Internet and of its uses by children.

c. Support regional and international capacity building efforts to improve policy and operational measures to protect children on the Internet, including the pooling and sharing of successful education and awareness raising tools.

d. Better co-ordinate work by the various international and regional organisations and bodies which play a role to support government efforts in this area, including OECD, Asia-Pacific Economic Co-operation, Council of Europe, European Union, Internet Governance Forum, ITU, Organisation of American States, and involve non-governmental stakeholders where appropriate.
6. **INVITES:**

- Members and the Secretary-General to disseminate this Recommendation to all stakeholders and other international organisations;
- Non-Members to adhere to this Recommendation and collaborate with Members in its implementation.

7. **INSTRUCTS** the Committee for Information, Computer and Communications Policy to review this Recommendation and its implementation and to report to Council within five years of its adoption and thereafter as appropriate.
OECD members are invited to answer this questionnaire on the implementation and continued relevance of the 2012 OECD Recommendation on the Protection of Children Online (Recommendation).

The Recommendation focuses on the protection of children as users of the Internet. It does not address child pornography or the sexual exploitation of children on the Internet. These topics were excluded on the basis that each requires radically different measures to protect children, and in some cases law enforcement cooperation such as through Interpol.

A key question in this review, is whether the online risk typology has changed since the Recommendation due to children's increasingly constant access to and use of the Internet through mobile apps and devices. Respondents are asked to consider whether the typology of online risks developed in the background report (2011) are still appropriate to the current online environment. The typology (Figure 1) includes content risks, contact risks, risks related to children as consumers as well as information security and privacy risks faced by children on the Internet.

Figure 1. Typology of risks
General information

a. Country
b. Coordinator(s) contact details

1. Implementation and enforcement
   1. Does your country have laws and regulations intended to protect children online?
      1.a) If yes- please provide references to the most relevant laws and regulations
   2. Does your country have a policy/policies intended to protect children online?
      2.a) If yes please provide references to the most relevant policies.
   3. Which bodies/agencies are responsible for the enforcement of these laws and regulations?
   4. Please provide any additional relevant information
   5. Does your country address cross-border issues with the exception of child pornography which require international coordination?
      5.a) If yes - please provide examples
   6. Does your country implement educational initiatives to build children’s resilience against online risks?
      6.a) If yes - please provide examples
   7. Does your country organise awareness-raising events/campaigns?
      7.a) If yes - Please provide examples (e.g campaigns on the occasion of the Safer Internet Day [insert link to https://www.saferinternetday.org/])

2. Leadership and responsibility
   1. What agencies or ministries are involved with developing and implementing children online policy?
      1.a) Please provide any additional relevant information
   2. What is the role of non-governmental stakeholders – including business and civil society – for developing and implementing children online policy?

3. Monitoring and evaluation of policies
   1. How do you measure the effectiveness of your policy/policies?
   2. Do you have monitoring of specific policy targets?
2.a) If yes - please provide policy target examples

3. What data and indicators are used to measure policy effectiveness?

4. How do you use the results from monitoring and evaluation to improve your children online policy?

5. Please provide any additional relevant information

4. Measuring online risks for children
   1. Which online risks for children are measured systematically in your country?
   2. Does the measurement allow comparison over time?
   3. If yes - are there any particular trends emerging from the evidence you collected since 2012?

5. Review of the 2012 Recommendation
   1. In light of developments since the adoption of the 2012 Recommendation, does your country consider the 2012 Recommendation still relevant?
      1.a) Please provide a short explanation of which developments are required to update the 2012 Recommendation
   2. Is the typology of online risks for children reproduced in the introduction still timely or in need of expansion to include new online risks?
   3. Which online risk categories should be addressed in a review, because they are new or require updated evidence?

Please rate on a sliding scale 1 to 6 (with 1 being low priority and 6 being high priority)

1. Internet addiction (e.g. clinical addiction to certain online activities)
2. Harmful overuse of connected devices and online services (e.g detrimental to children’s well-being)
3. Cybergrooming (e.g adult/ minor or minor/ minor entering into contact online with the aim to abuse)
4. Sexting (e.g minors voluntarily sharing intimate images with others)
5. Internet of Things (e.g. connected toys - physical toys connected to the Internet)
6. Children online privacy (e.g. online tracking and monitoring)
7. Harmful advise (e.g self-harm and suicide, pro-anorexia/ bulimia websites)
8. Bullying/ trolling and harassment (e.g posting inappropriate or embarrassing photos of others)
9. Radicalization (e.g extremist content)
10. Hateful content (e.g bordering to hate speech)
11. In-app purchasing (e.g coercive game purchasing practices)
6. Other
   1. Do any parts of the 2012 Recommendation (other than the principles) need to be changed?
      1.a) Please explain your responses and provide examples of possible changes
   2. Are there any principles that may require modification or deletion?
      2.a) Please explain your response, and indicate which principle(s) require modification or deletion
   3. Is there a need for new principles to be developed?
      3.a) Please explain your response, and provide examples of changes that could be made.
   4. Are there specific age thresholds in your country regarding the need for parental consent in the collection of personal data from children?

7. Relevant technological developments
   1. Are you aware of technological developments and innovation, such as parental controls, age verification, and other technical safeguards to protect children online?
      1.a) Please provide examples

End of questionnaire