



EUROPEAN COMMISSION

Brussels, 31.1.2012  
C (2012) 404 final

## **SAFER INTERNET**

**A multi-annual union programme on protecting children using the Internet and other  
communication technologies**

## **WORK PROGRAMME**

**2012**

## TABLE OF CONTENTS

1.	INTRODUCTION.....	3
2.	OBJECTIVES AND OVERALL APPROACH.....	4
2.1.	Safer Internet programme .....	4
2.2.	Participation in the Safer Internet programme.....	5
2.3.	International scope of the Safer Internet programme.....	6
3.	ACTION LINES 1 & 2 EUROPEAN NETWORK OF SAFER INTERNET CENTRES.....	7
3.1.	Action 1.1 Safer Internet Centres.....	7
3.2.	Action 1.2 Safer Internet Days 2012 and 2013 .....	13
4.	ACTION LINE 2 – FIGHTING AGAINST ILLEGAL CONTENT AND HARMFUL CONTACT AND CONDUCT ONLINE .....	14
4.1.	Action 2.1 Targeted project: Enhancing law enforcement agencies' identification and analysis of child pornography .....	14
5.	ACTION LINE 3: PROMOTING A SAFER ONLINE ENVIRONMENT .....	18
5.1.	Action 3.1 Thematic network: Promoting positive online experiences for young children.....	19
5.2.	Action 3.2 Follow-up to benchmarking study on filtering software and parental control tools.....	20
5.3.	Action 3.3 Benchmarking of Safer Internet policies in Member States and policy indicators.....	20
5.4.	Action 3.4 Safer Internet Forum .....	20
5.5.	Action 3.5 Encouraging self-regulatory measures in promoting a safer online environment for children.....	21
5.6.	Action 3.6 European coordination of stakeholder groups.....	22
6.	ACTION LINE 4: ESTABLISHING A KNOWLEDGE BASE.....	22
6.1.	Action 4.1 Knowledge enhancement project: investigating the impact on young people of convergence of technology .....	23
6.2.	Action 4.2 Knowledge enhancement project: Identifying child friendly search/browser tools.....	24
7.	EVALUATION PROCESS .....	25
7.1.	Appointment of independent experts for evaluation and reviews.....	25
7.2.	Eligibility criteria .....	25
7.3.	Award criteria.....	26

7.4.	Selection criteria.....	29
8.	IMPLEMENTATION PLAN AND BUDGET.....	30
8.1.	Call for proposals .....	30
8.2.	Public procurement .....	31
8.3.	Other expenses .....	32
8.4.	Indicative timetable for related activities.....	32

## 1. INTRODUCTION

The 2012 Safer Internet Work Programme sets out the priorities for activities to be funded under the Safer Internet programme<sup>1</sup>. In particular, the Work Programme describes the kinds of activities the 2012 call for proposals will cover, what its objectives are, the criteria for funding, the expected results, and the indicative budget, and provides information about events that the European Commission will organise in collaboration with the organisations funded.

This Work Programme also takes into account and implements policies laid down in the:

- Recommendation on the protection of minors and human dignity and the right of reply<sup>2</sup>
- Communication on the rights of the child<sup>3</sup>
- Communication on cybercrime<sup>4</sup>
- Charter of Fundamental Rights of the European Union<sup>5</sup>
- Council Framework Decision 2008/913/JHA on combating racism and xenophobia<sup>6</sup>
- UN Convention on the Rights of Persons with Disabilities<sup>7</sup>
- Audiovisual Media Services Directive<sup>8</sup>
- Communication on future networks and the internet<sup>9</sup>
- Digital Agenda for Europe<sup>10</sup>
- Communication on "e-Skills for the 21<sup>st</sup> Century"<sup>11</sup>
- Action Plan Implementing the Stockholm Programme<sup>12</sup>

---

<sup>1</sup> Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies, OJ 348, 24.12.2008 p. 118.

<sup>2</sup> Recommendation of the European Parliament and of the Council on the protection of minors and human dignity and the right of reply in relation to the competitiveness of the European audiovisual and information services industry (2006/952/EC), OJ L 378 , 27.12.2006, pp. 72-77.

<sup>3</sup> Commission communication 'Towards an EU Strategy on the Rights of the Child', COM(2006) 367 final.

<sup>4</sup> Commission communication 'Towards a General Policy on the Fight against Cyber Crime', COM(2007) 267 final.

<sup>5</sup> OJ C 364/01 of 18.12.2000

<sup>6</sup> Council Framework Decision of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328 of 6.12.2008, p. 55

<sup>7</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:023:0035:0061:EN:PDF>

<sup>8</sup> Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 amending Council Directive 89/552/EEC, OJ L332, 18.12.2007, p. 27.

<sup>9</sup> Commission Communication COM (2008) 594 final.

<sup>10</sup> Commission Communication COM (2010) 245 of 19.05.2010

<sup>11</sup> Commission Communication COM(2007) 496 of 07.09.2007

- Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography (repealing Framework Decision 2004/68/JHA COM(2010)94)<sup>13</sup>.

## **2. OBJECTIVES AND OVERALL APPROACH**

### **2.1. Safer Internet programme**

The Digital Agenda for Europe<sup>7</sup> foresees several key actions for children online. The overall context and aim is to make a better internet for children and the Commission's strategy is articulated round the following axes:

(i) awareness and empowerment - to provide children, their parents and teachers with the tools, knowledge and skills to use safely the internet, enjoy positive experience and behave and act responsibly online;

(ii) protecting youth on line - to prevent children from being exposed unnecessarily to harmful behaviours, contacts or content which can either be the cause of distressing experiences online or expose them to risks in the real world;

(iii) fighting illegal content - to increase speed of the notice and take down procedure of child pornography from the internet while allowing the police to lead an investigation against perpetrators, as well as to prevent re-upload and continued circulation of the images.

The overall aim of the Safer Internet programme ('the Programme') is to promote safer use of Internet and other communication technologies, to educate users — particularly children, parents and carers — in this regard, and to fight against illegal content and harmful conduct online.

The Programme runs for the five years 2009 to 2013. It has a budget of EUR 55 million to be spent on four action lines, set out as follows.:

Action line 1) ensuring public awareness

Action line 2) fighting against illegal content and tackling harmful conduct online

Action line 3) promoting a safer online environment

Action line 4) establishing a knowledge base.

It is implemented through annual Work Programmes.

In 2012, actions in all these areas will be implemented by means of: a call for proposals; public procurement actions; and the organisation by the Commission of a number of activities to bring together relevant stakeholders, such as organising awareness-raising and coordination activities both at the European level (Safer Internet Day, Safer Internet Forum, etc) and at the international level.

---

<sup>12</sup> Commission Communication COM(2010) 171 final

<sup>13</sup> [PE-CONS 51/11](#) of 4.11.2011

In 2012, there is a specific focus on ensuring the full geographical coverage of the Safer internet Centres' European network, on improving access to quality content for young children and on strengthening the existing technological capacity to deal with illegal content.

In addition studies on benchmarking of safer internet policies and evidence building will be carried out. Their results will feed into future strategy for making a better internet for kids and for the follow-up to the Programme from 2014 onwards.

Last but not least the Programme will keep its strong focus on children and youth's participation. Children are active and enthusiastic users of the internet and other online technologies such as mobile phones. The work of the Safer Internet programme is based on knowledge of how children use these technologies. Safer Internet Centres are required to involve children and young people in their work by setting up youth panels where young people can express their views and pool their knowledge and experience of using online technologies. Pan-European Youth Forums have been organised together with the INSAFE network in conjunction with the Safer Internet Forum since 2009. A pan-European Youth Forum may be held again in 2012.<sup>14</sup> Moreover in 2011 the European Award for Best Children's Online content included prizes for young creators (12-17 years old) of quality content for young children (6-12 years old). Youth participation in future editions of this competition will be further encouraged.

## **2.2. Participation in the Safer Internet programme**

Action 1.1 of the 2012 call for proposals will only be open for proposals for providing a Safer Internet Centre in the following countries: Cyprus, Czech Republic, Denmark, Estonia, France, Greece, Iceland, Italy, Latvia, Lithuania, Luxembourg, The Netherlands, Malta, Portugal, Slovakia, Sweden, United Kingdom and Russia<sup>15</sup>.

Participation in all other actions of the 2012 call for proposals is open to legal entities established in the Member States. Legal entities established in EFTA States which are contracting parties to the EEA Agreement (Norway, Iceland and Liechtenstein) may also take part.

Under the 2012 Workprogramme the following organisation and country are established as priority for international cooperation and therefore are entitled to receive funding:

- The international organisation INTERPOL is established as priority for co-operation in the field of fighting against illegal content. See Section 4.1.
- RUSSIA is established as a priority for co-operation in the field of ensuring public awareness and fighting against illegal content and harmful contact and conduct online. In particular legal entities from Russia can submit proposals to provide a Safer Internet Centre in this country. The funding will be limited to 100% of the costs of belonging to the network of Safer Internet Centres, unless Russia decides to join the Programme through signature of a bilateral agreement (See section 3.1). In addition legal entities from Russia may also take part in targeted projects, thematic networks and knowledge enhancement

---

<sup>14</sup> <http://eskills-week.ec.europa.eu>

<sup>15</sup> There are the countries for which a) the 2011 call for proposals was not open, b) no Safer Internet Centre was selected following the 2011 call for proposals or c) no Safer Internet Centre will be funded by the programme after 1<sup>st</sup> January 2014.

projects under the same conditions as entities established in Member States (but not as project co-ordinators).

Legal entities established in other countries may take part under the conditions set out in Article 2 of the Decision setting up the Programme<sup>16</sup>, provided that the country signs a bilateral agreement to join the Programme.

In addition, under Article 2(2) and Paragraph 3 of Annex III of the Decision setting up the Programme, Russia is established as a priority for international co-operation<sup>17</sup>.

Legal entities established in non-EU countries other than those referred to above and international organisations may take part in any project at their own expense, with the exception of INTERPOL, as mentioned above.

Up-to-date information about the countries currently taking part in the Safer Internet programme is available on the Programme web site at <http://ec.europa.eu/saferinternet>.

### **2.3. International scope of the Safer Internet programme**

The issues covered by the Safer Internet programme are global and need national, European and international solutions. This is particularly true for illegal content. Material depicting child pornography may be produced in one country, hosted in a second, and accessed and downloaded all over the world. Commercial payment systems operating worldwide may be used to fund the sale and purchase of the images.

Digital technologies offer an unprecedented means of facilitating freedom of expression and communication around the globe. As Internet access and mobile phone use become more widespread in Europe and in the rest of the world, children are increasingly becoming active users of the technology. Working with non-European countries may provide useful insights into the way in which children are using the technology and new ideas on how to equip them and their parents, carers and teachers with the necessary knowledge.

In 2012, international cooperation will focus on the following actions:

- involvement of as many third countries as possible in Safer Internet Day;
- participation of other European neighbouring countries at regional or international events organised by Safer Internet Centres;
- participation in international events such as the Internet Governance Forum and the ITU Child Online Protection (COP) initiative and co-ordination with relevant activities of International Organisations;

---

<sup>16</sup> Decision No 1351/2008/EC of 16 December 2008 of the European Parliament and of the Council, OJ 348, 24.12.2008, p. 118.

<sup>17</sup> See special conditions for participation of Russian legal entities in the network of Safer Internet Centres footnote 26. Russian entities may also take part in targeted projects, thematic networks and knowledge enhancement projects under the same conditions as entities established in Member States (but not as project co-ordinators).

- invitation to experts from countries outside the EU to Safer Internet events (e.g. Safer Internet Forum, European network meetings);
- exchange of best practices in fighting illegal content and awareness raising, including exchange schemes for experts or organisations from countries outside the EU.

### **3. ACTION LINES 1 & 2 <sup>18</sup> EUROPEAN NETWORK OF SAFER INTERNET CENTRES**

The Safer Internet programme will continue to fund the European network of Safer Internet Centres. Each Centre is national and Europe-wide networking between them is coordinated. The purpose of the network is to coordinate activities and bring together a variety of stakeholders to act and help transfer knowledge locally, regionally and throughout Europe. The project type of Safer Internet Centres described below is "Integrated network".

#### **3.1. Action 1.1 Safer Internet Centres**

Safer Internet Centres currently exist in all Member States, consisting of an awareness centre, and in most cases a hotline for reporting illegal content as well as a helpline aimed at providing advice and support to children and parents on online safety and concerns including grooming and cyberbullying .

In order to make best use of the available budget and to allow continued full geographical, funding will be made available in 2012 only for those countries listed in section 2.2.

##### *3.1.1. Common requirements*

All Safer Internet Centres will perform awareness-raising activities. In addition they should include (a) hotlines to which the public can report illegal content and/or (b) helplines where parents and children can obtain advice on how to deal with uncomfortable or scary experiences of using online technologies.

It is essential that a Safer Internet Centre exists in a country where a hotline or helpline is set up, to assist in ensuring visibility. No stand-alone hotline or helpline will be funded under the Programme.

In order to achieve maximum efficiency and impact, each component of the Safer Internet Centre (awareness-raising, hotline, helpline) should preferably consist of a single organisation. The same organisation can apply for more than one component. Where a consortium applies, the division of labour between the partners should be clear and logical. The recommended maximum size of a consortium for a Safer Internet Centre is up to four partners if a hotline and a helpline are included. If the consortium is larger, the Commission may require it to be cut down in size or offer a lower rate of funding. However, the Commission may approve additional strategic partners, not requesting funding, committed to specific project activities.

Only one Safer Internet Centre will be funded within a given country. A single grant will be given for a Safer Internet Centre.

---

<sup>18</sup> Action 1 of the Decision No 1351/2008/EC is "ensuring public awareness", action 2 is "fighting against illegal content and harmful contact and conduct online"

### 3.1.2. *Common tasks:*

The three components of the Safer Internet Centre will be expected to cooperate by:

- setting up a single Advisory Board with local stakeholders;
- setting up a Youth Panel;
- exchanging information about their respective activities;
- agreeing common positions on safer internet issues for submission to policy-makers and the media;
- running joint awareness raising activities/campaigns;
- contributing to the visibility of Safer Internet Day.
- ensuring that the information and communication developed in the actions conform to accessibility standards.

Proposals must:

- clearly describe the current situation in the country regarding issues related to safer use of the internet and other online technologies and demonstrate the value that the proposed Safer Internet Centre expects to add in this context;
- explain what support the project would receive from national authorities, industry, NGOs or childcare organisations and provide supporting letters from such organisations stating what kind of support they will give the project;
- show how the proposed Safer Internet Centre will cooperate with other organisations.

### 3.1.3. *Illegal vs harmful content, contact and conduct online*

The main form of illegal content covered by this Work Programme is child pornography. Another is racism and xenophobia. Europe-wide standards exist to combat both<sup>19</sup>.

Work in this area will be carried out in cooperation with DG HOME, in particular as regards the directive on child sexual abuse and sexual exploitation<sup>20</sup>.

For the purposes of this Work Programme, harmful contact refers to contact preparatory to committing a sexual offence against a child by contacting them online, sometimes referred to as ‘grooming’<sup>21</sup>.

---

<sup>19</sup> Council Decision of 29 May 2000 to combat child pornography on the Internet (2000/375/JHA), Council Framework Decision of 20 January 2004 on combating the sexual exploitation of children and child pornography (2004/68/JHA) and Council Framework Decision on combating racism and xenophobia (2008/913/JHA).

<sup>20</sup> Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography (repealing Framework Decision 2004/68/JHA COM(2010)94 of 29.03.2010), PE-CONS 51/11 of 4.11.2011

Harmful conduct refers to bullying and harassment in the online environment, so-called cyberbullying.

Harmful content is content which parents, carers, teachers and other adults responsible for children consider to be harmful to them. The concept of what is harmful also varies across countries and cultures. A variety of means exist to deal with harmful content, all of which need to be used in combination to increase their effectiveness: self-regulation and technical tools, awareness-raising, training and education, and enforcement of legal provisions, where they exist. Depending on national legislation some harmful content may also be illegal, in which case it may be subject of law enforcement measures..

Dealing with illegal content, harmful content, harmful contact and harmful conduct may require different methods, strategies and tools. However, some tools such as awareness-raising can be used for all categories.

#### *3.1.4. Awareness-raising*

Since 2004, the Safer Internet programme has been promoting awareness in a co-ordinated way across the European Union through the European network of awareness centres. The awareness centres' main aim is to develop awareness raising material, organize campaigns and information sessions for children and young people, parents, carers, social workers and teachers to enable children and young people to make responsible use of on-line technologies.

Safer Internet centres promote public awareness by conveying a positive message about the opportunities of a wider and more intensive use of information and communication technologies while providing adequate information about risks and ways to deal with them.

The awareness actions address issues related to harmful content, contact and conduct. They also address the opportunities and risks of services using new distribution forms, such as peer-to-peer services, broadband video, instant messaging, chat-rooms, social networking sites and access to content and interactive information and communication brought about by the rapid take-up of internet, mobile phones and game consoles by children. They take into account the related issues of protection of privacy and personal data, consumer protection, information, and network security (viruses/spam).

#### **Tasks for awareness-raising:**

Safer Internet Centres will coordinate and carry out awareness actions and programmes in close cooperation with all relevant actors at European, regional and local levels.

- devise inventive, attention-grabbing and informative awareness campaigns using the most appropriate media, taking into account best practice and experience in other countries, which may involve the participation of children and young people;
- promote awareness of parents and children on online positive content and experience and pay particular attention to awareness raising actions towards young children and children at risk;

---

<sup>21</sup> This is the process by which abusers target children through the relative privacy of the Internet and mobile phones by sometimes pretending to be children themselves and by befriending vulnerable children online.

- take into account the results of research and knowledge-enhancement projects funded by the Safer Internet programme;
- inform the intended target groups about other activities funded by the Safer Internet programme<sup>22</sup>,
- use cost-effective means of distribution of information to large numbers of users (multiplier organisations, electronic dissemination channels, mass media, information material distributed to schools and to internet cafés);
- evaluate the impact of the awareness campaigns on the target groups and provide qualitative and quantitative feedback at European level on the national achievements to improve the impact and effectiveness of the European network;
- establish and maintain formal or informal partnerships and promote dialogue and exchange of information with key players (government agencies, press and media groups, ISP associations, user organisations, education stakeholders) and actions in their country on to safer use of the internet and other online technologies;
- actively cooperate with other Safer Internet Centres in the European network by exchanging information about best practices, participating in meetings and designing and implementing a European approach;
- take an active part in European-level events and in the organisation of regional and local events for Safer Internet Day;
- where appropriate, support preparations for the Safer Internet Forum by holding national events on the topics to be discussed there;
- where appropriate, cooperate with other actions under the Safer Internet programme;
- where considered appropriate by the European Commission, cooperate with non-EU countries by exchanging information about best practices, sharing awareness tools, participating in international meetings, and hosting visits.

#### **Conditions for awareness-raising:**

Bodies seeking to carry out awareness-raising tasks as Safer Internet Centres need to show that they have strong support from national authorities. They should have a clear mandate to educate the public in safer use of the internet and other online technologies or in media and information literacy.

#### *3.1.5. Hotlines*

Hotlines allow members of the public to report illegal content and pass the reports on to the appropriate body for action (Internet Service Provider (ISP), the police or a corresponding hotline). Hotlines do not investigate offences or arrest or prosecute offenders. They may represent centres of expertise regarding illegal material and child pornography in digital media, providing guidance to ISPs and other stakeholders as to what content might be illegal

---

<sup>22</sup> Including hotlines, helplines, self-regulation schemes and the SIP BENCH II study on benchmarking the effectiveness of parental control software and services

in a country. Close cooperation with the national law enforcement agencies is an important element of the hotline operation.

As an alternative to establishing or running a hotline as part of the Safer Internet Centre, the Centres may enter into an agreement with a national alert platform to publicise that platform and include a link to it on their web pages.

### **Tasks for hotlines:**

- establish and/or operate a hotline to receive information from the public relating to illegal content<sup>23</sup>;
- draw up a manual of procedures in cooperation with law enforcement authorities and in accordance with best practice guidelines;
- actively inform users of the hotline’s remit and how to contact it;
- deal rapidly with complaints received;
- undertake a preliminary assessment of the legality of the content reported and trace its origin;
- forward the report to the appropriate body for action (police, ISP, correspondent hotline);
- conduct systematic notice to the host service provider of content assessed as child pornography, in accordance with the manual of procedures, and to monitor the time span needed to take down such content;
- contribute to the European URL database run by the network co-ordinator and provide statistics required for measuring the impact and effectiveness of the European network;
- actively support the further development of the tasks and competencies of the International Association of Internet Hotlines (INHOPE) as suggested by the European Commission;
- participate actively in networking with other local stakeholders;
- take part in cross-border discussions and exchange of best practice with other co-funded hotlines, and with other stakeholders as part of the network.

### **Conditions for hotlines:**

The hotline may be either public or private or a public-private partnership. A public hotline may be run by the police or by another public body, provided that it is prepared to cooperate with other hotlines which are part of the network, whatever their status.

The hotline must certify that it is able to cover the full range of hotline tasks.<sup>24</sup>

---

<sup>23</sup> Funding of hotlines under this Work Programme is exclusively for work assessing reports dealing with child abuse images or racism and xenophobia.

<sup>24</sup> If a hotline cannot demonstrate that it is able to cover the full range of hotline tasks the Commission may consider to cut the funding earmarked for the hotline within the Safer Internet Centre, or to not fund the hotline at all.

The hotline should show that it has the necessary support for its activities from national authorities and law enforcement agencies and that its activities will be in accordance with EU law and national law, including data protection rules.

The work of the hotline should support and be integrated in the system set up in accordance with the Council conclusions of 24 October 2008 on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet<sup>25</sup>.

### *3.1.6. Helplines*

Safer Internet Centres should establish or cooperate with helplines from which parents and children can obtain advice on how to deal with harmful contact (grooming), harmful conduct (cyberbullying), harmful content and uncomfortable or scary experiences of using online technologies,

The helplines may also take reports on grooming and cyberbullying and forward them to the appropriate body for action. These tasks could be carried out by two different organisations within a Safer Internet Centre

#### **Tasks for helplines :**

Helplines should carry out the following tasks:

- offer one-to-one conversations with trained helpers in real time (online and by telephone)
- answer online questions and telephone calls from children and parents related to their use of online technologies;
- design operating guidelines and a training module for the staff in compliance with national law, including data protection rules;
- have in place a system for passing reports to the relevant authority where a child appears to be in danger;
- actively inform the users of the helpline’s remit and how to contact it;
- draw up safety tips after consulting stakeholders and researchers;
- disseminate the results by providing statistics on the number of calls/contacts received and the issues raised;
- discuss the results of its activities within the Safer Internet Centre and give input to awareness raising strategies;
- participate in networking at European level and contribute to cross-border discussions and exchange of best practices.

#### **Conditions for helplines:**

---

<sup>25</sup> 2899th Justice and Home Affairs Council meeting, Luxembourg, 24 October 2008.

Setting up a helpline should be done in conjunction with organisations with the necessary experience and infrastructure, such as organisations currently running helplines dealing with calls/contacts from children.

### *3.1.7. Funding:*

Safer Internet Centres will receive up to 50% of eligible costs (which may be increased up to 75% for public bodies, SMEs and non-profit organisations)<sup>26</sup>.

## **3.2. Action 1.2 Safer Internet Days 2012 and 2013**

Safer Internet Day, initiated by the European Commission, is part of a global drive by awareness-raising partners to promote a safer internet for all users, especially young people. Celebrated under the patronage of the Commissioner for Information Society and Media, since 2005 Safer Internet Days have been organised by the European internet safety network INSAFE, co-funded by the Safer Internet programme, involving a broad number of organisations and countries across Europe and worldwide.

Since the first edition, participation in this event has been steadily growing, with an increase in general awareness, stronger involvement of relevant stakeholders in the field of internet safety and a high level of media interest.

In 2011, more than 65 countries all over the world participated in Safer Internet Day. In 2012 work will continue to involve an even larger number of participants in Safer Internet Day activities in an even greater number of countries. The INSAFE network of awareness centres will develop a toolkit that would help all interested stakeholders to participate in Safer Internet Day activities. The Commission may organise a central event to promote Safer Internet Day.

Safer Internet Day 2012 will take place on Tuesday 7 February 2012 and will focus on the topic of connecting generations and discovering the digital world together..

Preparatory work for Safer Internet Day 2013 will start in 2012.

## **4. ACTION LINE 2 – FIGHTING AGAINST ILLEGAL CONTENT AND HARMFUL CONTACT AND CONDUCT ONLINE**

A central aim for the Safer Internet programme is to reduce the amount of illegal content trafficked online and to deal adequately with harmful contact and conduct, with a particular focus on online distribution of child pornography, grooming and bullying.

In addition to providing funding for a European network of hotlines, to ensuring coverage of hotlines and helplines throughout the Member States (see action 1.1 above Safer Internet Centres), in 2012 the programme will provide funding for a targeted project to supply police investigators with tracking tools and access to aggregated intelligence allowing more efficient

---

<sup>26</sup> If a Safer Internet Centre is selected for Russia, in the absence of a bilateral agreement, the funding will be limited to 100% of direct eligible costs of taking part in the networking activities of Safer Internet Centres.

identification of child victims and consumers of child pornography in the EU Member States and third countries.

The programme will continue to coordinate its activities in the field of illegal content and awareness-raising with DG HOME and DG JUSTICE.

#### **4.1. Action 2.1 Targeted project: Enhancing law enforcement agencies' identification and analysis of child pornography**

The Programme invites proposals for a single targeted project to

##### **(1) Complement the existing International Child Sexual Exploitation database by setting up an international child pornography database with video images and by deploying it (area 1)**

While the International Child Sexual Exploitation (ICSE) database<sup>27</sup> is successfully establishing its status as the international focal point for victim identification investigations in this crime area, there is one core key functionality which is lacking and increasingly desired by police investigators - the database is limited to images and neither allows the aggregation of video evidence material nor offers tools to analyse video images.

Currently, in the EU, there are hardly any video databases on child pornography on a national basis.<sup>28</sup> Where such databases exist they are neither accessible on a transnational level nor do they use technologies which would allow the matching of content. The aim of the projects is to examine, collect and aggregate such content in one database which would be made accessible to EU Member State law enforcement agencies and to law enforcement agencies of other countries interested in using it.

Objectives for area 1:

In addition to the common requirements for targeted projects<sup>29</sup>, proposals should be aimed at the following:

- (a) The establishment of a database which would gather intelligence on child victims of sexual abuse, namely child pornography in the form of video images, which is currently dispersed across law enforcement agencies in several countries;
- (b) The development or enhancement of technological tools for the specific needs of the police, facilitating the analysis of evidence material gathered in the database across different formats. The tools would help linking different pieces of evidences together, such as video images of the same victim or perpetrator and of crime scenes; it would allow identifying and distinguishing new material from already known material. It would allow matching details across the video images database and the images stored in the ICSE database. This

---

<sup>27</sup> At INTERPOL

<sup>28</sup> The Dutch police are working on such a national database, using the latest technologies (the video fingerprint technology developed under the I-Dash project, funded under the SIP, which allows matching videos across different formats).

<sup>29</sup> See point 4.1.1 below

would namely enable facilitation and widening of investigations in order to rescue the victims from the abusive situation. Existing technologies such as "video fingerprints" would be used as far as available or be further developed if necessary;

- (c) EU Member States and third countries where critical masses of child pornography on the internet is being identified would be connected and given access to the database. Corresponding training of dedicated law enforcement investigators would be included. At least 20 EU Member States should be connected and benefit from training.

**(2) Set up a set of search tools (for content tracking) apt for the different protocols of Peer2Peer networks and establish an international Peer2Peer database; deploy the tools by connecting EU Member States and other countries (area 2)**

Peer2Peer stands for 70% of all internet traffic. EUROPOL estimates that the biggest share of non-commercial dissemination of child pornography happens there.

Currently, there are some law enforcement agencies in EU Member States which already use existing tools for tracking child pornography in selected Peer2Peer networks. However, the data which they gather are scattered across mostly local, in some cases also regional or national databases and the available tool set does not allow tracking such content across all Peer2Peer networks in operation. This area therefore has three main goals: enhance the gathering of data concerning the exchange of publicly accessible child pornography in Peer2Peer networks in one international database, thus aggregating evidence data; gather the existing tracking tools in one tool set and complement the tool set for such Peer2Peer networks not yet covered, thus enabling investigations across multitudes of Peer2Peer networks; and allow a single access point for dedicated law enforcement agencies. The data tracking tools shall not allow opening or examining communications; data to be gathered shall only that which are publicly available.

Objectives for area 2:

In addition to the common requirements for targeted projects<sup>24</sup>, proposals should be aimed at the following:

- (a) Software deployment and development: It would gather already existing software systems based on hash codes which work on different Peer2Peer protocols (such as eDonkey, Gnutella etc.). Some software (for Peer2Peer networks not yet covered) would be developed;
- (b) Software development should also cover the areas of Usenet / newsgroups and internet relay chat (IRC);
- (c) The system should be easy to use and to connect via web services. It should allow sufficient hundreds of connections to take place at any one time;
- (d) An international computer infrastructure would be established, accessible for dedicated law enforcement agencies which gives law enforcement access to the tools they need to leverage the latest technologies to identify and track those

who query for or who offer child pornography on Peer2Peer networks, Usenet and IRC;

- (e) The database would gather the evidence which will be produced by law enforcement working with the tools offered, thus aggregating intelligence in one international database;
- (f) EU Member States and third countries where critical masses of child pornography on the internet is being identified would be connected and given access to the database, provided they can ensure the necessary safeguards. Corresponding training of dedicated law enforcement investigators would be included. At least 20 EU Member States should be connected and benefit from training.

**(3) Develop a pilot to test trusted hash code / fingerprint series for preventing re-uploading of identified child sexual abuse material (area 3)**

The hash codes of images and "fingerprints" of videos (as stored in the ICSE international database and in national databases) can be used for further purposes: for developing a pilot tool which could be taken up by industries (namely ISPs, file hosters<sup>30</sup> and Social Networking Sites) to remove, to prevent re-uploading and for tracking child pornographic content being exchanged in Peer2Peer networks.

The main goal of this work package is to create a guaranteed secure tool applicable only to known child pornography content, which would allow industries to move from reactive (i.e. the take – down of identified child pornography) to a pro-active policy; it is expected that this would reduce the amount of child pornography being stored, hosted, transmitted or re-uploaded to their networks.

The tool would integrate a security mechanism against its and the data set's unlawful use by third parties.

Objectives for area 3:

In addition to the common requirements for targeted projects<sup>24</sup>, proposals should be aimed at the following:

- (a) The establishment of a set of verified child pornographic images and videos - the images would stem from a law enforcement database and they would be regarded internationally as illegal child pornographic material. An infrastructure would be set up which facilitates the continuous updating of the set.
- (b) The development or enhancement of a technological tool which would help industries to prevent their networks from being misused for storing, hosting, transmitting or the re-uploading of known child pornography. The tool would be based on hash code, photo DNA, video fingerprint technologies or related

---

<sup>30</sup> IWF and the jugendschutz.de hotlines report that the amount of child abuse images and videos uploaded to file / image / video hosters is being significantly increasing.

technologies which are already available.. The application of the tool by industries is voluntary and must respect EU and national law

- (c) The set of child pornographic images and videos will be made available to law enforcement agencies in the EU Member States and internationally for the purpose of investigations and / or for cooperation with industries. This would include the development of guidelines and user-briefing. The system must ensure that the material is only accessible to authorised and trained personnel and is appropriately protected against any kind of misuse or unauthorised access or distribution.

### **Conditions for areas 1-3:**

- (a) Proposals must address all 3 areas;
- (b) Proposals are invited from national law enforcement agencies, international law enforcement organisations, research institutions (public and private), technology suppliers and engineering companies with expertise in the relevant fields of technology;
- (c) Proposals must be submitted by a consortium which includes at least two national police bodies (i.e. law enforcement agencies, police academies, police universities or ministries) from 2 different EU Member States.

As for area 3 at least two companies representing the ISP, Social Networking Services or file hosting sector must be either partners of the consortium or be involved indirectly, for instance through a project advisory board or a pilot user group, and accompany the implementation of this third area.

#### *4.1.1. Conditions*

Proposals for targeted projects may be submitted by a consortium of legal entities.

The issues addressed should have a European dimension, and the ways proposed to tackle them at European level should impact a large number of users in the largest possible number of EU countries.

Proposals should provide a clear description of the current underlying knowledge/state-of-the-art. As far as the expected impact is concerned, the target users and their needs, also beyond the consortium participants, must be clearly identified.

Proposals should also specify the sustainability of the proposed solutions. The results of the project must be made accessible to the public or relevant stakeholders beyond the end of the project. Exploitation and/or dissemination plans are expected to adequately support these objectives. Appropriate measures and indicators are required for monitoring the progress of the project and for assessing the results and impact of the activities.

The European added value of the proposal will have to be clearly demonstrated, including coverage of several different Member States. A targeted project consortium should be of a manageable size - an indicative size would be 3-8 applicants.

The potential end users / target group should be involved indirectly, for instance through a project advisory board or a pilot user group, to be consulted by the consortium in order to

provide advice and feedback on the results. At least 3 Member States should be involved as end users / target group.

Any proposal must comply with EU and national laws applicable to data protection and fundamental rights.

#### *4.1.2. Funding:*

Targeted projects will receive up to 50% of eligible costs (which may be increased up to 75% for public bodies, SMEs and non-profit organisations).

## **5. ACTION LINE 3: PROMOTING A SAFER ONLINE ENVIRONMENT**

The Safer Internet programme aims to bring stakeholders together to find ways of promoting a safer online environment and protecting children from content that parents, carers, teachers and other adults responsible for children consider harmful (see Section 3.2).

### **5.1. Action 3.1 Thematic network: Promoting positive online experiences for young children**

Based on the input of the EC focus group on positive content which in 2009 and 2010 gathered around 20 European stakeholders in this field there are some innovative initiatives like browsers for children and white lists at national level, but currently there are very few links among stakeholders at European level.

A first attempt to raise visibility on quality online content for young children has been the pilot competition in the period October 2010-June 2011. National competitions have run in 14 countries mobilising producers and experts in this field. The European Awards were given by Vice President Neelie Kroes in June 2011, in the framework of the Digital Agenda Assembly.

In 2012 work to roll over the competition in all European countries may start with the support of INSAFE and its members.

The topic of positive online experience and how to expand national approaches to a European level will be also discussed with relevant stakeholders at the Safer Internet Forum 2011 in October 2011.

As an additional step, the Programme invites proposals to set up a Thematic network for promoting positive online experiences for young children.

Thematic networks bring together stakeholders to ensure action throughout Europe and to facilitate coordination and knowledge transfer between countries.

Tasks:

a) Exchange good practices, issues and challenges in provision of content to young children, including the business model and make recommendations to enhance production and dissemination of positive content across Europe (including localisation). This activity will include a discussion forum gathering producers and providers in a dialogue on online content for children.

b) Discuss feasibility and requirements of a safe browser for kids / collation of white lists including suggestions on moderation and rating of websites for children. Requirements should take into account accessibility needs of disabled children. Please note that new or enhanced technical solutions in this area will not fall under this thematic network. They will be explored by a knowledge enhancement project (see section 6.2).

c) Make proposals for the roll over of a European wide competition.

d) Provide a report with overview on the market for positive content for children in Europe.

#### *5.1.1. Conditions:*

- The network should consist of public and private producers of online content for children and gateways (browsers/white lists), researchers, parents associations
- Membership should cover the majority of EU Member States and should be open and proactive in attracting new partners;
- The coordinator of the consortium must convincingly show that it has support from the other members of the network by, for example, providing letters of support.

The issues to be discussed and the aim of the actions of the thematic network must be clearly identified. Proposers must present an analysis of the impact of the actions under the thematic network. Appropriate measures and indicators for monitoring the progress of the project and for assessing the results and the impact of the activities are required. The links foreseen to be established with relevant external organizations or projects have to be described.

#### *5.1.2. Funding*

The costs of the network coordinator for coordinating and implementing the network are covered at a rate of up to 100% of direct eligible costs (as defined in the model grant agreement), excluding indirect costs (overheads). Network members cover their own running costs except travel to network meetings, which may be reimbursed under the network budget

### **5.2. Action 3.2 Follow-up to benchmarking study on filtering software and parental control tools**

Technical tools can help parents decide what types of content they would prefer their children not to see. The SIP-BENCH II study funded by the Safer Internet programme is the only comprehensive study of filtering software and services carried out at European level which takes into account the specific needs and concerns of European parents. The results of the first benchmarking cycle were released on 13 January 2011.

Since both the software and services available and the types of harmful content will evolve, it is necessary to ensure that information continues to be available and is regularly updated. A call for tenders will therefore be published for a follow-up study.

### **5.3. Action 3.3 Benchmarking of Safer Internet policies in Member States and policy indicators**

In order to give a complete overview of the European landscape regarding online safety, the Commission will put in place benchmarking of safer internet policies and actions across

Europe including an analysis of the current resources used for these activities and their breakdown between the Commission on one hand and Member States, the private sector and the voluntary sector on the other hand, and assess the scope for increasing the latter. The results will feed into the implementation of the Programme and into the preparation of the follow-up to the Programme.

#### **5.4. Action 3.4 Safer Internet Forum**

The open meeting of the Safer Internet Forum is a yearly event covering all Safer Internet actions, facilitating discussion and exchange of information, experiences and best practices at expert level and giving relevant national and European stakeholders a platform to drive consensus, recommendations, guidelines etc. It also provides an opportunity to discuss ways in which industry can contribute to ensuring the online safety of children and young people. The results and findings of ongoing and completed projects co-funded by the programme will feed into the process.

In 2012, the Safer Internet Forum will be held again in conjunction with the pan-European Safer Internet Youth Panel. The Forum will include parallel sessions organised by Safer Internet projects with the aim of finding next challenges that need to be tackled in the field of child online safety that could feed into the content of a new Safer Internet Programme to cover the period from 2014 onwards.

In 2012, the Safer Internet Forum may be uplifted and expanded to include higher level representations and more third country participation. It would then provide a platform for strengthening the existing cooperation to make the Internet a better place for kids.

#### **5.5. Action 3.5 Encouraging self-regulatory measures in promoting a safer online environment for children**

A fully functioning system of self-regulation is an essential element in limiting the flow of harmful and illegal content through online technologies<sup>31</sup>. Many self-regulatory initiatives concerning the protection of children in the online environment exist throughout Europe. However, as new technological possibilities and services emerge, both uses and risks change. In order to ensure the safety of children in the changing online environment, industry self-regulation needs to be encouraged and effectively monitored.

One of the important tasks of the European Commission is to gather stakeholders in order to exchange experiences and best practices and to create cooperation. As a result of this activity, two industry self-regulatory agreements have been signed<sup>32</sup>:

- The European Framework on Safer Mobile Use by Younger Teenagers and Children, signed on Safer Internet Day 2007.
- The Safer Social Networking Principles for the EU, signed on Safer Internet Day 2009.

---

<sup>31</sup> See the indicative guidelines for the implementation, at national level, of a self-regulation framework for the protection of minors and human dignity in online audiovisual and information services in the Council. Recommendation of September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, OJ L 270, 7.1.1998, p. 48.

<sup>32</sup> [http://ec.europa.eu/information\\_society/activities/sip/self\\_reg/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm)

Children go online younger and younger, with 38% of 9-12 year olds who use the internet having a profile on social networking sites. At the same time, youngsters do not use only PCs anymore to go online, but increasingly more often laptops, mobile phones, game consoles and other mobile devices that allow them to go online anywhere, anytime, away from parental supervision. Emerging services (such as location-based ones) may lead to new risks.

Therefore, the Commission launched a review of the current self-regulatory framework for the protection of children when using new technologies to look at new developments and challenges brought about by changing patterns of technology used by children, as well as at how these could be best responded to in order to ensure the empowerment and protection of minors when using new technologies.

In 2011 several multi stakeholders meetings took place to discuss self-regulation. In 2012 multi-stakeholders meetings are also foreseen to follow up on the review of the self-regulatory framework, and on the monitoring of its implementation, including through support to establishing the Coalition of CEOs.

### **Monitoring the effectiveness of European self-regulatory agreements**

On the basis of the European Framework on Safer Mobile Use by Younger Teenagers and Children, national codes have been signed in 25 Member States. In 2008, 2009 and 2010 the European mobile industry association GSME has published implementation reports of the national codes by mobile operators and the Commission continues to follow the development on the national and European level closely. In 2011 and 2012 the Commission continues to follow up on these developments and support dialogue and implementation of concrete safety measures.

In June 2011 the European Commission has published the first batch of findings of a second independent assessment of the implementation of the Safer Social Networking Principles for the EU. The results of the assessment show that progress has been made in implementing the self-regulatory agreement since 2010. However, more needs to be done, especially in areas such as ensuring minors' privacy.

The Commission will continue to encourage industry self-regulation and public-private partnerships and will continue to support the monitoring of the existing agreements. Therefore, more multi-stakeholders meetings are foreseen in 2012.

### **5.6. Action 3.6 European coordination of stakeholder groups**

The Commission will continue to ensure coordination of different stakeholder groups through:

- a Coordination Group representing the co-ordinators of all networks co-funded by the Programme (European network of Safer Internet Centres, NGO network, EU Kids Online network of researchers)
- a number of thematic Focus Groups including representatives of Safer Internet projects and other stakeholders, such as industry, parents' associations, teachers' representatives etc

The Coordination Group is chaired by the European Commission and meets twice a year, indicatively in March/April and September/October. It allows a structured exchange of information on ongoing and planned activities, and discussion of scope for joint actions.

The Focus Groups are convened by the European Commission and meet as required. The Commission may be assisted by experts brought in on contracts.

## **6. ACTION LINE 4: ESTABLISHING A KNOWLEDGE BASE**

The Safer Internet programme aims to establish a knowledge base for dealing adequately with existing and emerging uses of the online environment and relevant risks and consequences, with a view to designing adequate actions aimed at ensuring online safety for all users.

Knowledge enhancement projects are projects to strengthen the programme's knowledge base on safer Internet and online technologies generally. Following consultation of Safer internet stakeholders, under the 2012 Work Programme, the 'knowledge base' action will focus on the following topics:

- Understanding the impact on young people of convergence of technology
- Identifying Child-friendly Search tools

### **6.1. Action 4.1 Knowledge enhancement project: investigating the impact on young people of convergence of technology**

Internet provides children with new opportunities to play, learn, and be creative, to participate, communicate with people from all over the world and express themselves. The EUKidsOnline survey<sup>33</sup> shows that children start using new technologies from a very young age, not only from computers but from a more and more diversified range of connected devices. While new technologies bring a wide range of opportunities to children, they also carry some risks.

This is why the 2012 Work Programme calls for a knowledge enhancement project which should investigate through a quantitative and qualitative methodology how the changing conditions of access and use (mobile devices) bring greater or lesser risks to children's safety.

Proposals for training and education, awareness and mediation strategies to children's parents and professionals working with children should also be included in the project.

The results of the project should be made available in order to provide topics for further actions and studies.

#### *6.1.1. Conditions*

Proposals for the above mentioned knowledge enhancement project may be submitted by a consortium of legal entities. They should involve 3-4 Member States (geographically balanced). In addition, other countries may participate in accordance with point 2.2 of the 2012 Work Programme.

Proposals will be expected to clearly describe

- the current underlying knowledge and research on which they build

---

<sup>33</sup> [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20\(2009-11\)/EUKidsOnlineIIRreports/D4FullFindings.pdf](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20(2009-11)/EUKidsOnlineIIRreports/D4FullFindings.pdf)

- make use of methodology (qualitative and quantitative) and work plan appropriate to the proposed objectives, including their applicability in practical terms, for example staff expertise relevant to carrying out the project (e.g. their expertise in handling sensitive situations and issues) and how focus groups will be selected and approached and give their consent to the study at hand, taking into account the possible sensitivity of the subject to be investigated.

The European added value of the proposal must be clearly demonstrated, i.e. how the expected results will be of use to and might reflect a wider European situation and/or provide cross-border cooperation within the project.

The links foreseen to be established with relevant external organizations or projects have to be described.

The results must be made accessible to the public and relevant stakeholders beyond the end of the project. Exploitation and/or dissemination plans are expected to adequately support these objectives. Appropriate measures and indicators are required for monitoring the progress of the project and for assessing the results and impact of the activities.

#### 6.1.2. *Funding*

Knowledge enhancement projects will receive up to 100% of direct eligible costs (as defined in the model grant agreement), excluding indirect costs (overheads).

### **6.2. Action 4.2 Knowledge enhancement project: Identifying child friendly search/browser tools**

Just as in the offline world, as children are more vulnerable to risks, adults (parents, teachers, industry representatives, NGOs, public authorities) have to find the right balance between education and empowerment on one side and protection on the other.

This balance is especially important as very young children and teenagers have different needs when it comes to their online safety. Very young children rely much more on protection. Therefore the Programme encourages the creation of "online playgrounds" for younger children.

At the moment, appropriate multilingual search/browser tools for content suitable for children are not sufficiently available. Most of the search systems are designed for adults: they return information that is unsuitable for children, present information in lists that children find difficult to manage and make it difficult for children to identify the relevant parts.

This is why the 2012 Work Programme calls for a knowledge enhancement project which should identify the technical capability for being able to find content suitable for children and make it available through child-friendly search/browser tools.

The project should include the issue of continuous quality control of the content provided to children and provide an EU gateway to good content from trusted tools and sources.

#### 6.2.1. *Conditions*

Proposals for the above mentioned knowledge enhancement project may be submitted by a consortium of legal entities.

They should involve 3-4 Member States. In addition, other countries may participate in accordance with point 2.2 of the 2012 Work Programme. The European added value of the proposal must be clearly demonstrated, i.e. how the expected results will be of use to and might reflect a wider European situation and/or provide cross-border cooperation within the project. The issues addressed should have a European dimension, and the ways proposed to tackle them Europe-wide should benefit a large number of people in the largest possible number of EU countries.

The links foreseen to be established with relevant external organizations or projects have to be described.

Proposers should provide a clear description of the relevance and expected impact of the subject chosen, and of the current underlying knowledge and research on which it builds, making use of methodology (qualitative and/or quantitative) appropriate to the proposed objectives.

The results must be made accessible to the public and relevant stakeholders beyond the end of the project. Exploitation and/or dissemination plans are expected to adequately support these objectives. Appropriate measures and indicators are required for monitoring the progress of the project and for assessing the results and impact of the activities.

#### 6.2.2. *Funding*

Knowledge enhancement projects will receive up to 100% of direct eligible costs (as defined in the model grant agreement), excluding indirect costs (overheads).

## 7. EVALUATION PROCESS

### 7.1. Appointment of independent experts for evaluation and reviews

The evaluation of proposals will be based on the principles of transparency and equal treatment.

The Commission will appoint independent experts to assist with the evaluation of proposals and with the review of project results. The experts will be identified on the basis of a call for expressions of interest. Experts will be selected according to the skills and knowledge appropriate to the tasks assigned to them, taking into account the thematic requirements of the call or project, and considering geographical and gender balance.

Each submission will be assessed on the basis of the evaluation criteria, which are divided into three categories: eligibility criteria, award criteria, and selection criteria. Only proposals meeting the eligibility criteria will be evaluated further. These criteria are set out below.

### 7.2. Eligibility criteria

On receipt, all proposals and applications will be subject to an eligibility check, to ensure that they meet the requirements of the call, and of the submission procedure.

The following checks will be carried out:

- receipt of proposal by the Commission on or before the deadline date and time set in the call;
- proposal completeness: proposals which are substantially incomplete — i.e. do not include sufficient information to identify the partners, their legal status and their ability to carry out the work and to evaluate the scope of the proposed project — will be excluded.

Applicants will be excluded from participation if:

- a) they are bankrupt or being wound up, are having their affairs administered by the courts, have entered into an arrangement with creditors, have suspended business activities, are the subject of proceedings concerning those matters, or are in any analogous situation arising from a similar procedure provided for in national legislation or regulations;
- b) they have been convicted of an offence concerning their professional conduct by a judgment which has the force of *res judicata*;
- c) they have been guilty of grave professional misconduct proven by any means which the contracting authority can justify;
- d) they have not fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which they are established or with those of the country of the contracting authority or those of the country where the grant agreement is to be performed;
- e) they have been the subject of a judgment which has the force of *res judicata* for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;
- f) they are currently subject to an administrative penalty referred to in Art. 96(1) of the Financial Regulation;
- g) they are subject to a conflict of interest;
- h) they are guilty of misrepresentation in supplying the information required by the contracting authority as a condition of participation in the procurement procedure or fail to supply this information.

All applicants must declare on their honour that none of the above situations apply to them.

Applicants found to have made false declarations face financial penalties or exclusion from grants and contracts<sup>34</sup>.

### **7.3. Award criteria**

The relative merit of the proposals received will be judged on the basis of award criteria subject to specific weightings. There are separate sets of award criteria, with specific weightings for each network and project type.

---

<sup>34</sup> Article 175 of Commission Regulation (EC, Euratom) No 2342/2002 as amended by Commission Regulation 1248/2006 of 7 August 2006, OJ L 227/3 19/8/2006.

The award criteria are applied to the information supplied in the proposal. Each criterion is marked from 1 to 10. A maximum of 100 points can be attributed to a proposal.

Proposals that fail to obtain at least 60 points in the evaluation will not be selected for co-funding.

### 7.3.1 Integrated networks (Safer Internet Centres)

#### **1. Relevance, impact and quality of the technical part of the proposal (Weighting: 20%)**

- Contribution to achieving the objectives of the Safer Internet programme and the relevant action as set out in the call.
- Clear description of the current situation in the country regarding issues related to the use of Internet and other online technologies
- Proposed solutions and the intended impact of the Safer Internet Centre.
- Adequacy of the methodology and work plan for achieving the objectives stated in the proposal.

#### **2. Partnership, resources, management (Weighting: 35%)**

- Adequacy of the partnership in terms of relevance and expertise of the applicant organisation(s), size of the consortium, combination of complementary expertise and task distribution among the participants.
- Extent to which the project provides for the human and financial resources necessary to carry out the proposed work.
- Adequacy of the management and decision-making structures, communication flow and cooperation mechanisms within the Safer Internet Centre.

#### **3. National cooperation (Weighting: 30%)**

- Extent to which the project convincingly demonstrates support from national authorities, industry, NGO, and childcare organisations in the form of letters from them stating what kind of support they will give.
- Extent to which the Safer Internet Centre includes a hotline and a helpline.
- Cooperation with other organisations active in the field, both those funded by the Safer Internet programme and others.

#### **4. European added value and network contribution (Weighting: 15%)**

- European dimension of the issue(s) addressed, and extent to which the proposed action would contribute to tackling them at European level.
- Contribution of the Safer Internet Centre to the consolidation and further development of the European network.

### 7.3.2 Targeted projects

#### **1. Relevance and impact (Weighting: 30%)**

- Contribution to achieving the objectives of the Safer Internet programme and the relevant action as set out in the call.
- Expected impact of the proposed action.
- Adequacy of the exploitation and/or dissemination plans to ensure optimal use of the project results, also beyond the participants in the project.
- Description of how fundamental rights would be respected.

#### **2. Quality of the technical part of the proposal (Weighting: 30%)**

- Clear description of the current underlying knowledge/state-of-the art.
- Clear description of the problems addressed and the proposed solutions.
- Adequacy of the methodology and work plan for achieving the objectives stated in the proposal, including their applicability in practical terms (e.g. how possible target groups will be selected, approached, and give their consent to the proposed solutions).

#### **3. Partnership, resources and management (Weighting: 20%)**

- Quality of the partnership in terms of relevance and expertise of the applicant organisation(s), size of the consortium, combination of complementary expertise, and task distribution among the participants.
- Extent to which the project provides for the resources necessary for carrying out the proposed work.
- Adequacy of the management and decision-making structures, communication flow and cooperation mechanisms within the consortium.

#### **4. European added value (Weighting: 20%)**

- European dimension of the issue(s) addressed, and extent to which the proposed action would contribute to tackling them at European level.
- European added value of the consortium behind the proposal.

### 7.3.3 Thematic networks

#### **1. Relevance and impact (Weighting: 25%)**

- Contribution to achieving the objectives of the Safer Internet programme and the relevant action as set out in the call.
- Expected impact of the proposed action.
- Adequacy of the dissemination plans to ensure optimal use of the project results, also beyond the participants in the project.

#### **2. Quality of the technical part of the proposal (Weighting: 30%)**

- Clear description of the problems and the proposed solutions.
- Adequacy of the methodology and work plan for achieving the objectives stated in the proposal.

#### **3. Resources and management (Weighting: 20%)**

- Quality of the coordinating team and partnerships to achieve the coordination envisaged, adequacy of the management and decision-making structures, communication flow and cooperation mechanisms within the network and resources available.
- Adequacy of the measures and indicators for monitoring progress and assessing results and impact.

#### **4. Quality of the proposed network and European added value (Weighting: 25%)**

- Adequacy of the organisations participating in the network in terms of relevance, competences, combination of complementary expertise.
- European added value of the network.
- Links with relevant external organisations or projects.

### 7.3.4 Knowledge enhancement projects

#### **1. Relevance and impact (Weighting: 30%)**

- Contribution to achieving the objectives of the Safer Internet programme and the relevant action as set out in the call.
- Expected impact of the proposed action.
- Adequacy of the exploitation and/or dissemination plans to ensure optimal use of the project results, also beyond the participants in the project.

#### **2. Quality of the technical part of the proposal (Weighting: 30%)**

- Clear description of the current underlying knowledge/research.
- Clear description of the problems addressed and the assessment/study/survey to be undertaken.
- Adequacy of the methodology and work plan for achieving the objectives stated in the proposal, including their applicability in practical terms (e.g. how possible target groups will be selected, approached, and give their consent to the study at hand).

#### **3. Partnership, resources and management (Weighting: 20%)**

- Quality of the partnership in terms of relevance and expertise of the applicant organisation(s), size of the consortium, combination of complementary expertise, and task distribution among the participants.
- Extent to which the project provides for the resources necessary for carrying out the proposed work.
- Adequacy of the management and decision-making structures, communication flow and cooperation mechanisms within the consortium.

#### **4. European added value (Weighting: 20%)**

- European dimension of the issue(s) addressed, and extent to which the proposed action would contribute to tackling them at European level.
- European added value of the consortium behind the proposal.
- Links with relevant external organisations or projects.

### 7.4. Selection criteria

The selection criteria are designed to ensure that the applicants possess the resources to co-finance the project and the professional competencies and qualifications required to complete the work successfully.

The selection criteria are applied to the information supplied in the proposal. If this identifies cases of weak financial capacity or professional competency it may require compensating actions such as financial guarantees or other actions. Successful proposals leading to negotiations will be the subject of formal legal and financial validation as a prerequisite to the signing of a grant agreement.

The selection criteria are divided into two parts:

#### Financial and operational capacity to carry out the project

- Capacity to co-finance the proposed project as demonstrated by the applicant's accounts.
- Capacity to allocate adequate human resources to carry out the project in question.

## Professional competencies and qualifications

Documented relevant experience in the field of the proposed action.

## **8. IMPLEMENTATION PLAN AND BUDGET**

### **8.1. Call for proposals**

A single call for proposals, with a fixed deadline, will be published in 2012 covering the actions of the Programme.

#### *8.1.1. Budget*

The Union contribution to the indirect actions selected from the call for proposals 2012 will be covered by commitment appropriations for 2012, for which an indicative amount of EUR 13.422.200 is available<sup>35</sup>.

Grants for proposals submitted in response to this call will be awarded under grant agreements.

The evaluation of proposals will give rise to a list of proposals to be funded. This list may be complemented by a reserve list of proposals of sufficient quality to be funded if the budget is available.

Within the indicative budget for the call, changes not exceeding 15% of the maximum contribution of the Union are not considered to be substantial provided that they do not significantly affect the nature and objective of the Work Programme.

#### *8.1.2. Project overview*

	<b>Characteristics</b>	<b>Duration</b>	<b>Co-funding rate</b>	<b>Typical consortium size</b>	<b>Indicative EU contribution (€)</b>	
<b>Integrated network</b>	Safer Centres awareness hotlines and helplines	Internet — raising, and	Up to 28 months	Up to 50-75% co-funding of eligible costs	3-4 partners for Safer Internet Centres <sup>36</sup>	10.872.200
<b>Targeted project</b>	Enhancing enforcement agencies' identification	law and	Up to 36 months	Up to 50-75% co-funding of	3-8 partners	1.000.000

<sup>35</sup> Under the condition that the draft budget for 2012 is adopted without modifications by the budgetary authority.

<sup>36</sup> The Commission may approve additional strategic partners, not requesting funding, committed to specific project activities.

	analysis of illegal material		eligible costs	
<b>Thematic network</b>	Promoting positive online experiences for young children	24-30 months	Up to 100% funding of a limited set of direct eligible costs	At least 10 partners/members 450 000
<b>Knowledge enhancement projects</b>	Investigating the impact on young people of convergence of technology	Up to 24 months	Up to 100% funding of direct eligible costs	3-4 partners 1.100 000
	Identifying child friendly search tools			
<b>TOTAL</b>				<b>13.422.200</b>

## 8.2. Public procurement

An indicative amount of EUR 1 550 000 is available<sup>37</sup> for the following public procurement procedures planned in 2012:

<b>Title</b>	<b>Indicative date for launch of procedure</b>	<b>Indicative budget (€)</b>
Expenses for Safer Internet Day 2012 (1-2 public procurement contracts/framework contracts)	1st , 2nd, 3rd and 4th quarters	190 000
Follow-up to benchmarking study on filtering software and parental control tools	1st quarter	350 000
Benchmarking of national safer internet policies actions and policy indicators (1 public procurement/framework contract)	1st quarter	500 000
Support for Safer Internet Forum (up to 10 public procurement contracts)	2nd quarter	450 000

<sup>37</sup> Under the condition that the draft budget for 2012 is adopted without modifications by the budgetary authority.

Follow up of industry self-regulatory agreements (1-2 public procurement contract/framework contracts)	2nd quarter	60 000
<b>TOTAL</b>		<b>1 550 000</b>

### 8.3. Other expenses

An indicative amount of EUR 110 000 is available<sup>38</sup> for the following other activities planned in 2012:

<b>Title</b>	<b>Indicative date for launch of procedure</b>	<b>Indicative budget (€)</b>
Project reviews (+/- 16 appointment letters selected on the basis of the call for experts published in the OJ C130 of 9.6.2009, p.5)	1st , 2nd, 3rd and 4th quarters	60 000
Focus groups (up to 50 experts to be reimbursed)	1st , 2nd, 3rd and 4th quarters	50 000
<b>TOTAL</b>		<b>110 000</b>

The **indicative breakdown** of the 2012 budget<sup>39</sup> is as follows:

1. Ensuring public awareness 45%
2. Fighting against illegal content and tackling harmful conduct online 35%
3. Promoting a safer online environment 13%
4. Establishing a knowledge base 7%

### 8.4. Indicative timetable for related activities

<b>Date</b>	<b>Event</b>
December 2011	Adoption of Work Programme
January 2012	Publication of call for proposals
End of March 2012	Deadline, call for proposals
Mid April 2012	Evaluation
May 2012	Evaluation report approved by Authorising Officer (Directorate) and Draft Implementation Plan approved by

<sup>38</sup> Under the condition that the draft budget for 2012 is adopted without modifications by the budgetary authority.

<sup>39</sup> using the categories set in the breakdown of Annex II of the programme decision see fn. 1

	Authorising Officer (DG)
June 2012	Committee opinion on implementation plan
July-August 2012	Adoption of award decision
September-December 2012	Grant agreement signature

## **FURTHER INFORMATION**

For further information about this programme please consult the Safer Internet web site at <http://ec.europa.eu/saferinternet>.