European Commission

Information Society and Media Directorate-General

Content

Safer Internet *plus* programme

GUIDE FOR PROPOSERS

Part B

Combined Safer Internet and Awareness Nodes

July 2006

http://ec.europa.eu/saferinternet

Part B – AWARENOD - Description of content

This form is for use by proposals for combined safer Internet nodes (the merge of hotline & and awareness node into a single node) and awareness nodes (with or without helpline) only.

Awareness nodes interested in applying to run **helplines** (action 4.2) should include work package 9 in the work description. Combined safer Internet nodes should include work packages 5 and 6, which refer to hotlines only.

All pages must be numbered and should be headed with the project acronym chosen for the proposed project.

Title page

Use the title page format appended. Insert the project acronym, title and the country being applied for.

Content list for Part B

A standardised set of objectives, tasks, performance indicators and deliverables will be used for awareness nodes and hotlines. Therefore, no other information than the targets should be added to the work packages.

1. PROJECT SUMMARY

A brief note of not more than 4000 characters summarising the main features of the proposal:

Objectives

Work Packages

Milestones and deliverables

Resources (partner skills, support from non-partners). A**ny documented support from third parties (public and/or private bodies) should be attached to the proposal.**

Use the project summary format appended.

2. PROJECT DESCRIPTION

2.1. Rationale and objectives

In this section, use the standardised set of objectives.

2.2. Baseline and results

This section, which should not exceed 3 pages, should describe the current situation (state of the art) in the relevant area(s) including clear demographic information relevant for the action and then particularly the number of young people in the country. The section should describe the project's impact and the expected viability of the actions beyond the project phase. The project should further be justified in the context of other related national or European developments and activities. Applicants which intend to continue an existing action co-funded by the Safer Internet Action Plan should also provide details of their current achievements.

Use the project description format appended.

3. DESCRIPTION OF THE CONTRACTOR(S) AND RESOURCES

3.1 Description of single partner or consortium

A description of the participating organisation(s) and the area of expertise not exceeding 2 pages and in case of a consortium explaining their respective roles and how they complement each other. Combined nodes should add a description of overall co-ordinator, technical co-ordinator for hotline, technical co-coordinator for awareness and technical co-ordinator for helpline where appropriate). The applicants should also describe the tasks foreseen for subcontractors, if any.

3.2 Description of key personnel

Short curriculum vitae of the key persons to be involved in the project indicating relevant experience, expertise and involvement in other relevant (industrial, national or international) projects. Each CV should comprise no more than 10 lines. The description should also include details of the project team in terms of tasks and time commitments.

3.3 Financing plan

Applicants have to document by filling in the Financing Plan how they intend to provide co-financing for the project. This co-financing can be in the form of own resources, financial transfers from third parties or revenues generated by the project.

3.4 Management

A description, not exceeding 2 pages, of how the proposed action will be managed by the beneficiary/consortium, the decision making structures, the communication flow within the consortium, the quality assurance measures that will be implemented and how conflicts will managed.

Use the description of the contractor format appended.

4. PROJECT WORKPLAN

This section consists of three parts and it describes the work planned in order to achieve the objectives of the proposed action. **The tasks are already established by the Commission and no additional information should be added apart from the targets required in some of the work packages.**

4.1 Work Package Overview

Use the work package overview format appended.

4.2 Work Package Description

This section describes the different work packages (WPs) in the proposal . In total there are nine standard WPs, indicating the relevant tasks, expected results/indicators and deliverables.

- Applicants interested in running only an awareness node have to include WPs 1,2,3,4,7,8.
- Combined nodes should include also work packages 5 and 6 relevant to hotlines.
- Awareness nodes applying to run also helplines should include work package 9 relevant to helplines,

One of the required tasks in work package description (WP 7) is to set up a structured method of concertation. This means that Safer Internet nodes will be required under their grant agreements to set up a structured method of concertation in accordance with the guidelines below.

The structured method of concertation is implemented by an Advisory Board (The national documents establishing or describing the method may use other terminology).

The Advisory Board is intended to act as a channel of communication among stakeholders and the Safer Internet nodes.

It should have a defined membership and meet regularly.

The Advisory Board could include representatives of:

– Ministries responsible for new media, police and education;

– Regulatory body responsible for new media;

– Police unit dealing with cyber-crime;

– Internet Industry association;

– Major communication service providers (Internet and mobile);

– Non-governmental organisations dealing with child welfare;

– University researcher into children's use of new media.

Where there is more than one Safer Internet node in a country, they must agree upon its membership and operation or adhere to a body set up by the authorities which includes all Safer Internet nodes and other stakeholders.

Use the work package description format appended.

4.3 Deliverables List

A list of deliverables should be supplied indicating the number, title, nature, dissemination level and the due date of the deliverable.

Use the deliverables list format appended, including, if appropriate, the deliverables concerning the Helpline.

5. EUROPEAN ADDED VALUE AND NETWORK CONTRIBUTION

This section not exceeding one page should identify which issue(s) at European level the proposal is addressing and explain how the node will contribute to the consolidation and further development of the European network.

Use European added value and network contribution format appended.

Portuguese Safer Internet project

SAFER INTERNET PLUS

Description of work

Annex I

Standard Work Packages & Deliverables

For Combined Safer Internet Nodes (merge of hotline & awareness node into a single node) or Awareness Nodes (with or without helpline) only

[PSI]

[Portuguese Safer Internet project]

[Portugal]

Project summary (maximum 4000 characters)

Portuguese Safer Internet (PSI) project aims to develop in Portugal a culture of awareness and social contribution to report illegal contents in the Internet, in order to minimize as far as possible the negative aspects of the generalization of Internet usage. The awareness node will educate and inform people how to protect themselves from the dangers of the Internet, as a preventive and awareness action, and the hotline will be a resource for citizens to report illegal or harmful contents. In more detail:

1. Awareness node

As an awareness node, the projects and actions developed under the objective to inform and educate citizens, not only in what concerns to the type and nature of dangers underlying the use of the Internet, but also to provide the means and instruments available to prevent those same dangers. The PSI project is ambitious in these objectives as it will try to implement actions and communication strategies in order to achieve as diverse target groups as possible. Mainly:

1) basic and secondary schools students and teachers;

2) higher education students and communities;

3) Media groups and general opinion makers;

4) SMEs

5) Home users.

2. Hotline

At a European and International level, the hotline service will build upon the experience of other hotlines, either by communicating to police force illegal content hosted in Portugal, or to inform other hotlines of illegal and harmful content hosted abroad. It will essentially be another resource of Inhope to achieve their objectives. With the project conclusion, Portugal will have a fully operational system that will try to achieve four main objectives:

1) Citizens to report illegal or harmful content (identifying themselves or in anonymity);

2) An analytical team to study and produce denouncing reports;

Project summary (cont.) (maximum 4000 characters)

3) A light communication process to report legally the content to police forces;

4) A commitment with Internet Service Providers to block content until judicial analysis is made and to adapt, if necessary, their common acceptable usage condition objectives.

In order to fulfill the PSI project objectives, the consortium was assembled having in mind that, in itself, it would be a decisive asset for the project success. The consortium is composed by:

1 – Knowledge Society Agency (UMIC) – a Public Institute of the Ministry of Science, Technology and Higher Education responsible for promoting, coordinating and implementing projects in the Information Society at large, thus including the key areas of e-Inclusion, e-Accessibility, e-Democracy, e-Procurement and the production of statistics and analyses in the usage of Information and Communication Technologies (ICT).

2 – DGIDC – Directorate-General for Innovation and Curricular Development – a central department of the Portuguese Ministry of Education, where the Task Force CRIE - Computers, Networks and Internet in Schools – operates, whose aims are the conception, development and evaluation of initiatives concerned with the use of ICT at schools and in the learning process.

3 – FCCN – Foundation for National Scientific Computing - is a private, non-profit institution, with public interest status. Since the beginning of its activities in 1987, it has contributed, with the help of universities and several R&D institutions, to the expansion of the Internet in Portugal. The main activity of FCCN is to plan, manage and operate the national research and education network (Rede Ciência, Tecnologia e Sociedade – RCTS), a high performance network for institutions with greater demands in communications which is a natural experimenting platform for advanced communications services and applications.

4 – MICROSFT – Microsoft in Portugal is represented by MSFT, Lda which is a subsidiary of the Microsoft Corporation. Microsoft in Portugal has a key role in the spread of information technology usage and the promotion of digital inclusion. Security is one of the areas where Microsoft has been working with public and private institutions to promote the safe usage of information technologies.

Project description

1. Rationale and objectives

– Act as node(s) of awareness (and hotline) network(s) in [*Portugal*]

– Devise a cohesive, hard-hitting and targeted awareness campaign using the most appropriate media, taking into account best practice and experience in other countries

– Establish and maintain a partnership (formal or informal) with key players (government agencies, press and media groups, ISP associations, users organisations, education stakeholders) and actions in their country relating to safer use of Internet and new media

– Promote dialogue and exchange of information notably between stakeholders from the education and technological fields

– Where appropriate, cooperate with work in areas related to the Safer Internet plus programme such as in the wider field of media and information literacy or consumer protection

– Inform users about European filtering software and services and about hotlines and self-regulation schemes

– Actively cooperate with other national nodes in the European network by exchanging information about best practices, participating in meetings and designing and implementing a European approach, adapted as necessary for national linguistic and cultural preferences

– Provide a pool of expertise and technical assistance to start-up awareness nodes (new nodes could be 'adopted' by a more experienced node)

– Take an active part in European-level events and in the organisation of national and local events for the Safer Internet Day

– Cooperate with the hotline present in the country, if any, and Europe Direct

Combined nodes (hotlines & awareness nodes with or without helpline) to add:

– Establish, if necessary, and operate a hotline for Internet users in [*Portugal*] to report illegal and harmful material and activities, so as to reduce the circulation of illegal content on the Internet

– Inform users of the hotline's scope of activity and how to contact it; Hotlines should make clear to users the difference between their activities and those of public authorities, and will inform them of the existence of alternative ways of reporting illegal content.

– Deal rapidly with complaints received, in accordance with best practice guidelines drawn up by the network and in cooperation with law enforcement authorities.

– Exchange specific information on identified illegal content with other members in the network.

– Participate actively in networking nationally and at European level and contribute to cross-border discussions and exchange of best practice.

– Cooperate with the awareness node present in the country and Europe Direct.

– Take an active part in events organised for safer Internet day at European, national and local level.

2. Baseline and results (maximum 3 pages)

Current situation in Portugal:

– Portugal, according to the population Censos 2001, has approximately 10 million inhabitants, of which 30% are under 24 years old and 38% are under 29 years old.

– In 2005, as reported in EUROSTAT, 42% of Portuguese households had access to a computer, 31% to the Internet and 20% to a broadband Internet connection. In what concerns usage, 40% of the Portuguese population had already used a computer and 32% the Internet. Between 2002 and 2005, these two indicators had an annual average growth of, respectively, 14% and 19%.Individuals in 16-24 years old group are the highest computer and Internet users.

– The main activities developed under Internet by the Portuguese population are: sending/receiving emails; searching for information and reading/downloading online newspapers and magazines.

– A large investment was made in equipping and connecting all the Portuguese schools in broadband to the Internet. The initiative "Schools, Teachers and Portable Computers" equipped 1.100 schools with 26.000 portable computers for teachers (around 11.600) and students (around 232.000) and promoted the use of ICT in learning processes. This initiative will certainly lead to a more effective use of the Internet in Portuguese schools. It is the right moment to continue developing efforts in order to raise awareness among educators and students for the safe use of Internet among children and youngsters in order to promote and protect their interests.

– A campaign addressed to youngsters must be implemented in order to make them aware of the benefits and risks of the Internet.

– The project builds on previous experience and resources, namely the participation of DGIDC/CRIE as the coordinator of a project in the previous edition of the Safer Internet Programme of the European Commission.

– Segur@net, the site developed within the mentioned project, will function as a reference site for schools, with the contribution of all partners, displaying information, contents and expertise on the benefits and risks of online technologies as well as examples of best practices and experiences in this field. It will provide effective guidance to teachers, students, parents and the society in general on how to avoid the risks, to take full advantage of the Internet and to develop youngsters' critical evaluation skills.

– Teacher training in the field of ICT is also another area that has received a large investment from the central services of the Ministry of Education, with more than 550 teacher trainers being prepared in the last school year.

– Measures have to be taken to develop youngsters' critical evaluation skills as well as parental supervision and to raise awareness for Internet safety procedures among teachers, contributing to a better and safer pedagogical use of the Internet by students and teachers, raising awareness for safety procedures while using ICT in a context of the big increase of Internet use during the last years, in schools, homes and public spaces.

- A set of awareness tools will be produced, namely posters, leaflets, brochures, pens, T-shirts, pendrives, to be distributed at schools, meetings, conferences an other events promoted by the partners.

- There are a reduced number of sites addressing the problems of Internet security. FCCN's Computer Security Incident Response Team (CERT.PT) – the only CSIRT operating in the country that is accredited by an international organization, already provides recommendations and best-practices, focused on a more technical audience, mainly Systems Administrators. We intend to make this Awareness Node convey these messages to other target audiences such as Students, Enterprises, Public Administration and Home Users.

- FCCN's CERT.PT has, through the use of its website, email and other means, disseminated relevant awareness information dealing with topics of information security in networks. It has also conducted (and will continue to conduct) training seminars for organizations that intend to establish incident response teams. FCCN has also been involved in dealing with the main ISPs in Portugal in a project called "ISP-Forum", seeking to find the main issues affecting Internet users today and adopting best practices to address them.

- Statistics and experience (within FCCN's CERT.PT, for example) indicate that the average citizen's degree of awareness on questions concerning computer and network security is very low. Although the Internet is widely used throughout the country in all fields of activity, there is still much work to be done in educating users on the perils of the Internet and how to use it safely.

Combined nodes to add:

- Portugal has transposed to its national law the relevant European directives concerning cyber-crime and electronic commerce.

- The existing specialised police unit for cyber-crime, child pornography, is the Polícia Judiciária Portuguesa – SICIT - http://www.pj.pt/htm/noticias/criminalidade_informatica.htm

- Means to facilitate reporting of illegal content on the Internet will be adopted to make the process of blocking the content and prosecuting their disseminators much more efficient, benefiting from the European Hotlines network.

- The hotline will cover the following types of illegal content: Child abuse images, criminally obscene content and criminally racist content.

Please note that core tasks of a hotline which qualify for Community funding do not include other types of content which may be contrary to law such as copyright infringement or spam (unless it is alleged to contain or to refer to illegal content).

– what Internet services does the hotline cover? The hotline accepts reports dealing with content on the following Internet services : **WWW, newsgroups and e-mail.**

– does a hotline operator analyse the original content referred to in reports received so as to make a *prima facie* assessment whether it is illegal content? Yes. By the end of the project it is expected that the hotline operator can make a *prima facie* of the contents denounced.

– does the hotline trace the apparent origin of the content reported? Yes.

– does the hotline have a written agreement with law enforcement authorities? The hotline is a member of a group set up by government Partners within this consortium (FCCN and Microsoft) who have established informal cooperation with key elements in Portugal's Polícia Judiciária – the national law enforcement agency responsible for computer and network related crimes – namely within SICIT, the agency's section specifically in charge of such investigations.

Description of the node(s)

Description of single partner or consortium (maximum 2 pages)

The consortium, with three public bodies and a private company, is prepared to implement a combined project of awareness node and hotline, which, by the entities nature, represents in itself an important asset for the project success.

Knowledge Society Agency – UMIC (http://www.infosociety.gov.pt/). The core function of UMIC in this consortium is to coordinate and supervise the PSI project implementation in all its components, awareness node and hotline, and in all its communication amplitude and potentialities, creating synergies and acquiring best practices, on behalf of the project objectives achievement.

UMIC is the Portuguese public agency with the mission of planning, coordinating and projects development in the areas of the Information Society, including those of electronic government. The Knowledge Society Agency mission has presently a reinforced relevance since the Portuguese Government Program for 2005-2009 established a Technological Plan as the keystone of the Government's economic policy. This plan consists on a set of related policies and transversal measures guided by a vision of transforming Portugal into a modern knowledge society. The Knowledge Society Agency operates within the Ministry of Science, Technology and Higher Education and represents Portugal in the i2010 High Level Group and other European Union committees and working groups.

DGIDC – Directorate-General for Innovation and Curricular Development / CRIE – Task Force of the Ministry of Education (http://www.crie.min-edu.pt/). This Task Force was created on the 1st July 2005 by dispatch of the Minister of Education. Its mission comprises the conception, development and evaluation of initiatives concerned with the computers, networks and Internet use in schools and in learning processes. The awareness activities for safer use of the Internet proposed by the Task Force CRIE will be present within all its activities and projects. Several projects are being undertaken within the framework of its mission, which supports ICT projects in schools, sustains the development of educational software and educational web contents, promotes teachers training courses in ICT, supports schools to integrate ICT in the learning processes and provides schools with portable computers according to a national call for tenders held in the first semester of 2006, aiming at reinforcing the penetration of ICT in schools.

FCCN - Foundation for National Scientific Computing (http://www.fccn.pt/). is a private non-profit organisation whose responsibilities, in addition to those defined by its charter, include managing and operating the Portuguese NREN - named Science, Technology and Social Community Network (RCTS), designed to be an infrastructure for data communication. For more than ten years FCCN has been operating the only Internet Exchange Point in Portugal, named GigaPiX, which connects nearly all operators in the country, and the registry service of .PT domains under the authority delegated by the IANA (Internet Assigned Numbers Authority). These roles give FCCN a privileged position in dealing with national ISPs and other relevant entities dealing with Internet services.

FCCN also manages the security service CERT.PT, a Computer Security Incident Response

Team accredited by the Trusted Introducer for Europe since 2004. CERT.PT has been actively involved in disseminating, through its web site and e-mail, best-practices, recommendations and security alerts and bulletins to the public in general, as well as handling and coordinating security incidents within its constituency – the Science, Technology and Social Community Network.

Microsoft main asset and contribution to this consortium is the support it can provide to enlarge the group of target audience for this important project. Its strong network connections can be used by the consortium to reach broader audiences like home users, companies from all sizes, public organizations, schools, press and others. Also an important contribution is the large amount of content that Microsoft has produced in Portuguese regarding Internet Safety. This content has been a reference in the past years and can now be integrated in the awareness node.
Other contributions are its capacity to bring in new ideas and to contribute to implement them. One other important contribution is the availability of the best assets that the company can offer to other consortium members to make the whole project and each working package a success.

Combined nodes to add:

Overall co-ordinator – UMIC will be the coordinating entity of Portuguese Safer Internet (PSI) project, with responsibilities in planning, management and reporting to the European Commission the overall project implementation. Among the responsibilities, defined in work packages, Knowledge Agency Society will act as node of the awareness network for Portugal and will set up and Advisory Board by establishing agreements with main stakeholders and other European Safer Internet Nodes.

Technical co-ordinator for the hotline - FCCN will be in charge of the technical co-ordination of the hotline, namely accepting reports of illegal content on the Internet, via web or telephone, integrating and coordinating with other Hotlines within Inhope, proceed with reports to local law enforcement agencies when the host of said illegal content is based in Portugal, as well as participate in promoting the Hotline's visibility throughout Portuguese society. The experience of CERT.PT in dealing with security problems within its network and its expertise in technical, operational and legislation fields will have a important added value.

Technical co-ordinator for awareness node - DGIDC/CRIE will contribute, as a central department of the Ministry of Education, to:

- Promote the involvement of already existing networks of teachers training, ICT Competence Centres that support schools ICT projects, Higher Education institutions that work directly with primary schools and teachers Training Centers in preparing awareness tools and methods for teachers training, and activities that can be held in schools with the participation of students;

- Disseminate among schools of the results and products accomplished within the development of these projects;

- Criss-cross ongoing ICT projects with Segur@net through the participation in events – conferences, meetings – organized by the projects developed by the Task Force CRIE in order to give visibility to the project.

Support the consortium partners in all national campaigns and actions of the awareness node.

Description of key personnel (maximum 10 lines for each CV)

UMIC:

Luís Magalhães is President of the Knowledge Society Agency (UMIC), Ministry of Science, Technology and Higher Education, Portugal, since July 2005; Member of the Lisbon Strategy and the Technological Plan Coordination Network; Member of the National IST RTD Directors Forum and of the i2010 High Level Group of the European Union; Full Professor at Instituto Superior Técnico (IST) of the Universidade Técnica de Lisboa (UTL), since 1993; Correspondent Member of the Lisbon Academy of Sciences since 1995. Formerly, he was the President of FCT – Science and Technology Foundation (the Portuguese Research Council) between 1997 and 2002; Member of the European Science Foundation Governing Council (2000-2002). He holds a PhD (1982) and MSc (1980) in Applied Mathematics from Brown University, USA, and an Electrical Engineer degree (1975) from IST.

Bruno Fragoso has a degree in Communication Sciences (2002), and is attending a master degree in "Audiovisual, Multimedia and Interactivity", in the Faculty of Social and Human Sciences – Universidade Nova de Lisboa. He works at UMIC – Knowledge Society Agency, since 2004, currently as project manager in e-democracy field, e-engagement and e-voting. He is also involved in a work group related with e-democracy, coordinated by the Portuguese Association for the Development of Information Society - APDSI.

CRIE:

João Correia de Freitas is at the moment the coordinator for the Task Force Computers, Networks and Internet at School, form the Ministry of Education, since it was created in 2005. He is a teacher at the New University of Lisbon, Faculty of Science and Technology – FCT-UNL (Department of Applied Social Sciences) for Educational Technology and Didactics. Between 1997 and 2003 he was responsible for uARTE, a unit from the Ministry of Science and Technology, which integrated the national programme *Internet at School* and was responsible for the promotion of the use of Internet for pedagogical purposes. Between 1988 and 1994 he was the coordinator for the node of the *Projecto Minerva* at the FCT-UNL. He was a teacher for basic and secondary education between 1979 and 1987. Biologist and PhD in Educational Sciences, his main interests are the educational use of computers, networks and specially Internet at school.

FCCN:

Pedro Veiga, has a degree in Electrical Engineering (1975) and a PhD on Electrical Engineering (1984) from the Technical University of Lisbon. He his a full professor at the Faculty of Sciences of the University of Lisbon since 1993, in the Informatics Department. He his Chairman of FCCN since 1997. He was Manager of the Information Society Operational Programme (2000-2002), a member of the Portuguese Task-force on the Information Society (1996-2000), Visiting Scientist at the JRC/Ispra (1989-1990). He is responsible for the .PT TLD, Portuguese representative at present at the MB of ENISA and at the GAC of ICANN.

Lino Santos graduated from University of Minho in 1995 in Systems Analysis and Computer Engineering. He attends a law-school post-graduation course. Since 1995 he works at FCCN in the coordination of several projects regarding security and computer networking such as connecting all Portuguese schools to the Internet, establishing wireless networks in all higher education institutions, establishing a CSIRT function to the community, or deploying VoIP

services to Universities.

Gustavo Neves studied Mathematics and Computer Science at University of Minho until 1999, at which point he went to work for FCCN in Software Development and Database Administration. From to 2003 to the present, he is a member of FCCN's Security Incident Response Team – CERT.PT, in incident handling, authoring guides for best-practices recommendations and scientific papers in the field of Internet Security. He also participates in European *fora* of Incident Handling Teams and collaborates with European research Projects in Network Security (GEANT2). He obtained a certification in Incident Handling through the European TRANSITS program and in Advanced Incident Handling through Carnegie Mellon University's Software Engineering Institute.

MICROSOFT

Marcos Santos, Security Lead in Microsoft Portugal - Marcos Santos is since July 2003, in charge of the Platform Strategy and leading the Security area in Microsoft Portugal, being since then responsible for all the activities relating to the Security of Microsoft in Portugal. Marcos Santos started to work in Microsoft in 1997 has a Product Manager of Internet Products and later led the team of product managers in Portugal. During his professional experience he had the opportunity to work in the support in Microsoft France. Marcos Santos has a degree in computer science by the University Nova de Lisboa and has made several certifications and trainings in the Kellogg School of Management and Imperial College of London.

Adelaide Franco, Industry Manager in Microsoft Portugal - Adelaide Franco is, since January 2004, Education Manager in Microsoft Portugal, particularly responsible for the deployment of different programs, such as Microsoft's Partners in Learning Program, and for the strategy and development of solutions suited to the education market. During her professional experience, she was part of the Portuguese Youth Institute direction board, in which, as a representative, she was a member of the National Committee for the programs Leonard, Socrates, Youth for Europe, among others. Adelaide Franco has a degree in Psychology, by the University of Lisboa, a master degree in Human Resources Policies and Management by ISCTE, and has a Diploma in Organizational Communication by Complutense Faculty of Madrid, among other certifications.

Financing plan

Indicate how the participating organisation(s) intend to provide co-financing for the project. The co-financing can be in the form of own resources, financial transfers from third parties or revenues generated by the project.

Coordinator (UMIC)

Source of funding	**Amount in Euro**
Contribution from own resources	56000
Contribution by other organisation (to be specified below)	0
Direct revenues expected from the project (to be specified below)	0
Contribution requested from the Commission	56000
Total	112000

Details on contributions by other organisations:

- The business model will be one of the first activities to be defined during the first quarter of 2007.

Details on direct revenue/receipts generated by the project:

Other applicants (DGIDC/ CRIE)

Source of funding	**Amount in Euro**
Contribution from own resources	150000
Contribution by other organisation (to be specified below)	0
Direct revenues expected from the project (to be specified below)	0
Contribution requested from the Commission	150000
Total	300000

Details on contributions by other organisations:

Details on direct revenue/receipts generated by the project:

Other applicants (FCCN)

Source of funding	**Amount in Euro**
Contribution from own resources	144324
Contribution by other organisation (to be specified below)	0
Direct revenues expected from the project (to be specified below)	0
Contribution requested from the Commission	144324
Total	288642

Details on contributions by other organisations:

Details on direct revenue/receipts generated by the project:

Other applicants (MICROSOFT)

Source of funding	**Amount in Euro**
Contribution from own resources	*
Contribution by other organisation (to be specified below)	0
Direct revenues expected from the project (to be specified below)	0
Contribution requested from the Commission	0
Total	0

Microsoft couldn't at this point add a precise value. This value will be determined when the 2007's budget comes out. This won't affect the values at this point of the application, because Microsoft monetary contribution is not eligible for UE funding.

Details on contributions by other organisations:

Details on direct revenue/receipts generated by the project:

Management (maximum 2 page)

The consortium was thought to involve each entity in the responsibility of an activity or group of activities and in the fulfilment of the project objectives. Nevertheless, all partners participate and give inputs to every planned activity. UMIC, as project coordinator, will supervise and guarantee the correct functioning of the consortium decision making workflow.

The decision making structure is thought to address in first place the problem or activity to be solved and carried out. When possible, the decisions will be assigned to the different partners according to their roles and know how. After the clear definition of the needs, all opinions and perspectives will be organized and a priority setting of sub-issues will be defined. For each sub-issue, a decision making grid-analysis will be defined considering each opinion: What are the positive and negative aspects? Who and what does it impact? How does it fit in long term goals? Based on this analysis, the best possible option will be chosen.

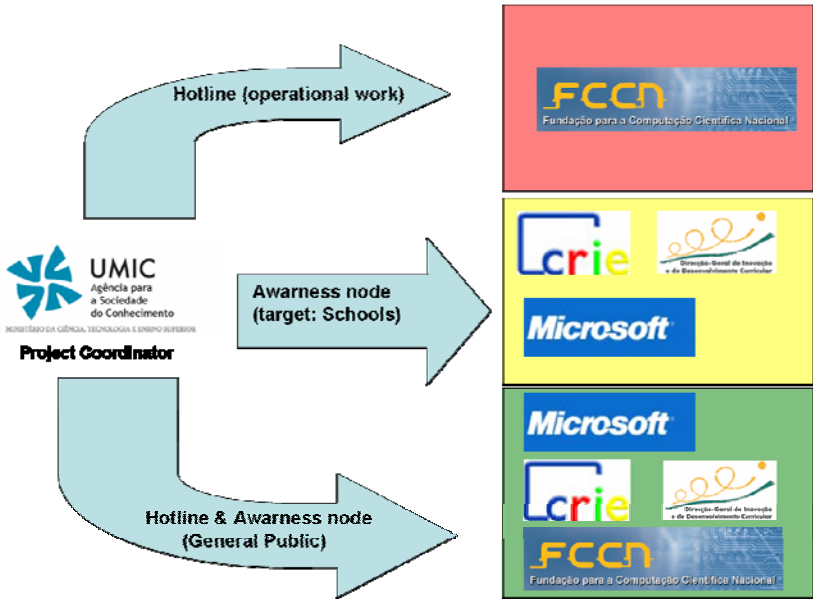
After the decision is taken and communicated to all partners of consortium, an action plan is drawn up, pointing clearly the steps/actions to take, the resources and people needed to implement the decision, a time schedule for each step/ action and the necessary ongoing assessment. For that, a specific set of measurable goals will be set, and a review of the decision implementation will be made periodically, making mid course corrections if and when necessary.

In order that the decision making structure works correctly, some communication workflows and communication instruments must be carefully selected and made operational. In the first quarter of 2007 the following aspects that support of the decision making model will be set:

- Periodical meetings with partners (in presence);
- Web based tools for sharing knowledge (reports, important documents, other relevant information);
- Periodical assessment reports for analyzing and evaluating the implemented actions efficiency.

In case of decision conflicts, UMIC's assumes the responsibility to unblock problematic issues, and to apply, if necessary, items prioritization and multi-voting to solve the problems and to define the next steps in a democratic way among the partners.

Previously to the submission of the PSI application to the European Commission, a Governance Model was set, in order to make clear the institutional relationships within the consortium:



Work Package Overview

Work-package No[1]	Work Package title	Lead Participant No[2]	Person-months[3]	Start month[4]	End month[5]
1.	Planning, management and reporting	UMIC	12	T0	T24
2.	Project assessment	UMIC	9	T3	T24
3.	Develop awareness tools and methods	CRIE	17	T0	T24
4.	Dissemination	UMIC	37	T0	T24
5.	Hotline operational work	FCCN	56	T0	T24
6.	Hotline visibility	UMIC	8	T0	T24
7.	National cooperation	UMIC	7	T0	T24
8.	Contribution to European network	UMIC	6	T0	T24
9.	Helpline (OPTIONAL)		-	T0	T24
	TOTAL		152		

1 Work package number: WP1 – WPn.
2 Number of the participant responsible for the work in this work package.
3 The total number of person-months allocated to each work package.
4 Starting date for the work in the specific work package, T0 indicates the start of the project and all other dates being relative to this date.
5 End date, T0 indicates the start of the project and all other dates being relative to this date.

Work Package Description (awareness node & hotline)

Work package number :	1	**Start date:**	T0	**End date:**	T24
Work package title:	Planning, management and reporting				
Applicants involved:	UMIC; FCCN; DGIDC/CRIE; MICROSOFT				
Person-months per applicant:	UMIC-5PM; FCCN-1PM; DGIDC/CRIE-5PM; MICROSOFT-1PM				

Objectives

Plan the work, monitor progress, supply periodic reports.

Tasks

1. Draw up a detailed work plan including mission statement, goals and operational objectives, resources and timetable.
2. Ensure that objectives, deadlines and quality standards are met. Establish adequate progress monitoring, assessment and quality control procedures through suitable indicators. Adapt project plan as required.
3. Liaise with EC project officer. Submit six-monthly progress reports, financial statements and an annual public report for publishing.

Expected results / indicators

Delivery on time of work plan and reports of satisfactory quality

Adherence to objectives, deadlines and quality standards

Deliverables

1. Management report covering the first three months of the project and including a detailed work plan for the future work
2. Six-monthly progress reports
3. Financial statements
4. Annual public report

Work Package Description (awareness node & hotline)

Work package number :	2	Start date	T3	End date:	T24
Work package title:	Project assessment				
Applicants involved:	UMIC; CRIE; FCCN; MICROSOFT				
Person-months per applicant:	UMIC-2PM; FCCN-1PM; DGIDC/CRIE- 5PM; MICROSOFT-1PM				

Objectives

Assessment of the work and of the results of the project. The assessment will be published.

Tasks

1. Draw up an assessment methodology providing for intermediate and final assessments
2. Carry out the intermediate assessment in accordance with the assessment methodology.
3. Carry out the final assessment as above.

Expected results / indicators

Appropriateness of assessment methodology
Degree to which assessment methodology is implemented
Timeliness and quality of assessments

Deliverables

1. Assessment methodology
2. Intermediate assessment report
3. Final assessment report

Work Package Description (awareness node)

Work package number :	3	**Start date:**	T0	**End date:**	T24
Work package title:	Develop awareness tools and methods				
Applicants involved:	UMIC; FCCN; DGIDC/CRIE; MICROSOFT				
Person-months per applicant:	UMIC-3PM; FCCN-5PM; DGIDC/CRIE-7PM; MICROSOFT-2PM				

Objectives

Devise a cohesive, hard-hitting and targeted awareness campaign using the most appropriate media, taking into account best practice and experience in other countries.

Tasks

1. Determine the specific objectives, appropriate 'marketing' strategies and effective messages for each target group.
2. Prepare a comprehensive set of awareness tools tailored to meet national needs (including information for users about European filtering software and services and about hotlines).
3. Identify key players (stakeholders, key industrial and institutional circles and multiplier organisations), contact them and ask them to participate. Organise preparatory meetings with key contacts at national level covering the different target audiences.
4. Identify upcoming events (seminars, conferences, discussion forums, theme- workshops, trade fairs, round tables, etc) Activities may be focused on one or several target groups at national/local level.
5. Design an Activity Plan including distribution of awareness tools and a mass media Communication Plan.

Expected results / indicators

Quality of awareness tools and appropriateness for target audience

Timely delivery and quality of Activity Plan and mass media Communication Plan

Number of stakeholders and multiplier organisations identified, contacted and agreeing to take part – **Target:**

- 21 ICT Competence Centres + 13 High Education Intitutions + 5 Regional Departments of the Ministry of Education;

- 20 relevant entities from Civil Society and Government in 2007 and 40 in 2008 (e.g. IAC [child support organization]; IPJ [young people organization] ; GNS [National Security Cabinet]; PJ [National Police]; Confap [Parents organization]);

Number of events identified - **Target:** 25 (e.g. National Security Day; Internet Safe Day; Teachers

events;)

Deliverables

1. Activity plan (included in the first six-monthly progress report)
2. Mass media Communication Plan (included in the first six-monthly progress report)
3. A set of awareness tools – **List:** E-mail distribution list, Set of good practice guides online, legal framework for network security, Website; posters; brochures; pens, T-shirts, leaflets, pen-drives

Work Package Description (awareness node)

Work package number :	4	**Start date:**	T0	**End date:**	T24
Work package title:	Dissemination				
Applicants involved:	UMIC; FCCN; DGIDC/CRIE; MICROSOFT				
Person-months per applicant:	UMIC-5PM; FCCN-4PM; DGIDC/CRIE-25PM; MICROSOFT-3PM				

Objectives

Act as node of the awareness network for [Portugal]

Tasks

1. *Implement the Activity Plan* Organise various awareness and dissemination activities geared towards the different target groups. Focus on training the trainers and other multiplier activities. Promote information literacy as well as information and discussion amongst national "specialists" in crucial areas and within target groups at the national level.
2. *Implement the mass-media Communication Plan.* Stimulate and coordinate media and press coverage and visibility, using different strategies, including: use of traditional media (press, radio, TV) to stimulate public awareness; send awareness packages to media and opinion leaders; use the editorial services of multiplier organisations to promote the dissemination of information (e.g. publication of articles in magazines, web sites, etc.).
3. *Organise high-profile events* including national, local events for Safer Internet Day and participate in key events identified under WP 2.
4. *Set up a project web site* where to find information regarding the activities of the awareness network and to download awareness tools. The web site should use a common European visual theme and have links to the network coordinator, the Safer Internet programme and other Safer Internet nodes in the country, if any.

Expected results / indicators

Number of tools distributed - **Target:** 5 000 posters; 25 000 leaflets; 25 000 brochures for students and teachers and 10 000 for general population.

Number of trainers trained - **Target:** 2000

Number of downloads of tools available online - **Target:** 3000

Number of TV/press/radio items and audience reached. - **Target:** 240 divided by in two years

Visibility of hotline among a specified relevant target population of the general public **Target:**

- 60% of population in academies and schoold and 40% in general public after 24th month.

Number of events organised, number of applicants - **Target:**

- 60 events – 10 000 people

Deliverables

1. Implementation of Activity plan (included in six-monthly progress reports)
2. Implementation of Mass media communication plan (included in six-monthly progress reports)
3. Project web site

Work Package Description (hotline)

Work package number :	5	**Start date**	T0	**End date:**	T24
Work package title:	Hotline operational work				
Applicants involved:	FCCN; UMIC; CRIE; MICROSOFT				
Person-months per applicant:	FCCN-53PM; UMIC-1PM; DGIDC/CRIE-1PM; MICROSOFT-1PM				

Objectives

Operate a hotline for Portugal to take reports of illegal content and/or activity on the Internet and new online technologies

Tasks

1. Set up and maintain a facility for online reporting of illegal content and/or activity on the Internet and new online technologies, including a Web site.
2. Establish and review operational procedures for dealing with reports on illegal content on the internet by forwarding them to the appropriate bodies for action and for appropriate treatment of reports outside the field of hotline activity
3. Receive, log and process reports in accordance with operational procedures
4. Operate the hotline in a user-friendly manner, including informing internet users about identifying illegal content and applicable law and providing feedback about the progress and outcome of their reports, where available
5. Recruit, train and supervise staff. Open a dialogue on staff welfare and find ways to achieve this
6. Implement and monitor compliance with best practice guidelines established by the network
7. Gather and analyse statistics based on the network template to track performance and establish trends

Expected results / indicators
Number of reports received **Target:** 5000
Web site: no. of pages, no. of hits **Target:** 1000 hits/site/day
Frequency that content gets removed
Number of guidelines implemented: Full process detailed in guidelines, since the report of content, until the judicial denounce.
Other indicators, in accordance with best practice guidelines to be adopted by the network and agreed upon by the Commission
Deliverables
1. Reporting facility, Web site
2. Operational procedures manual
3. Statistics based on the network template (to be included in the six-monthly progress report)

Work Package Description (Hotlines)

Work package number :	6	**Start date**	T0	**End date:**	T24
Work package title:	Hotline visibility				
Applicants involved:	UMIC; FCCN; CRIE; MICROSOFT				
Person-months per applican	UMIC-2PM; FCCN-4PM; DGIDC/CRIE-1PM; MICROSOFT-1PM				

Objectives

Ensure that the hotline is known both by decision-makers and relevant actors and by the general public

Tasks

1. Promote the hotline to decision-makers and relevant actors in key sectors (industry, police / public prosecutors, officials responsible for protection of minors, child welfare organisations)
2. Promote the hotline to the general public through use of multiplier organisations (Internet-based, broadcasting media and press, awareness projects, parents organisations etc)
3. Cooperate with the awareness node present in the country and Europe Direct.
4. Take an active part in events organised for Safer Internet Day at European, national and local level.

Expected results / indicators

Awareness of hotline among decision-makers and relevant actors

Number of press reports

Number and effectiveness of agreements with multiplier organisations

Visibility of hotline among a specified relevant target population of the general public **Target:** 60% of population in academies and school and 40% in general public after 24th month.

Deliverables
Visibility-enhancement plan (included in the first six-monthly progress report)
Visibility-raising activities (included in the six-monthly progress reports)

Work Package Description (awareness node & hotline)

Work package number :	7	**Start date:**	T0	**End date:**	T24
Work package title:	National cooperation				
Applicants involved:	UMIC; CRIE; FCCN; MICROSOFT				
Person-months per applican	UMIC-1PM; FCCN-2PM; DGIDC/CRIE-2PM; MICROSOFT-2PM				

Objectives

Ensure networking with relevant actors at national, regional and local levels

Tasks

1. Set up a structured method of concertation, implemented by an Advisory Board, with the relevant stakeholders. The advisory Board should act as a channel of communication among stakeholders and the Safer Internet node, have a defined membership and meet regularly. Where there is more than one Safer Internet node (e.g. a hotline) in a country, they must agree upon its membership and operation or adhere to a body set up by the authorities which includes all Safer Internet nodes and other stakeholders.

2. Ensure the involvement of a) suitable multiplier organisations to guarantee adequate coverage of the target audiences b) industry and bodies concerned with child welfare (including law enforcement, ISPs, content providers and aggregators from electronic publishing and audiovisual sectors, search engine providers, media regulators, official and voluntary bodies).

Combined nodes to add:

3. Cooperate with ISPs, content providers and law enforcement agencies.

Expected results / indicators

Number of organisations involved in structured method of concertation, level of activity / cooperation – **Target:** 20 organizations comprising ISPs, government and public administration bodies, law enforcement and industry;

Hotline - Number and appropriateness of formal agreements between hotlines and the relevant actors such as law enforcement, ISPs and content providers and other complaints-handling bodies.

Deliverables
1. Set up of structured method of concertation
2. Implementation of Structured method of concertation (included in six-monthly progress reports)
3. Understanding on cooperation with law enforcement agencies, ISPs and content providers

Work Package Description (awareness node & hotline)

Work package number :	8	**Start date:**	T0	**End date:**	T24
Work package title:	Contribution to European network				
Applicants involved:	UMIC; FCCN; DGIDC/CRIE; MICROSOFT				
Person-months per applicant:	UMIC-1PM; FCCN-2PM; DGIDC/CRIE-2PM; MICROSOFT-1PM				

Objectives

Contribute actively to the European network and cooperate with the coordinating node and other members of the network

Tasks

1. Actively cooperate with other national nodes in the European network by exchanging information about best practices, participating regularly in network meetings and designing and implementing a European approach, adapted as necessary for national linguistic and cultural preferences.
2. Take an active part in network events and organisation of national and local events for Safer Internet Day.
3. Take part in sharing expertise and technical assistance between nodes in the European network.
4. Share resources with other nodes especially regarding web content, newsletters, awareness tools, PR material and branding.
5. Participate in working groups established by the network

Combined nodes to add:

Exchange reports with other members of the network

Observe agreed best practices

Cooperate in training schemes and mentor programmes to exchange expertise between hotlines

Expected results / indicators

Number of days spent on European network activities (minimum 20 days per node) - **Target: 35**

Number of European network events attended by node representatives. - **Target: 10**

Number of resources shared - **Target: 2**

Deliverables

1. Participation in activities of European network (included in six-monthly progress reports)

List of Deliverables

No[1]	Deliverable title	Delivery date[2]	Nature[3]	Dissemination level[4]
D1.1	Management report including detailed work plan	T3	R	C
D1.2.A	Progress report including the activity plan and mass media communication plan	T6	R	C
D1.2.B	Progress report including visibility enhancement plan and hotline statistics	T6	R	C/P
D1.3	Six-monthly progress reports	T12, T18, T24	R	C
D1.4	Financial statements	T24	R	C
D1.5	Annual/final public report for publishing	T12, T24	R	P
D2.1	Assessment methodology	T3	R	P
D2.2	Intermediate assessment report	T12	R	P
D2.3	Final assessment report	T24	R	P
D3.3	Set of awareness tools	T1 - T24 according to detailed work plan	O	C
D4.3	Project web site	T3	O	P
D5.1	Web site and reporting facility for hotline	T3	S	P
D5.2	Operational procedures manual	T3	R	C
D7.1	Set up of structured method of concertation	T3	R	C
D7.3	Understanding on cooperation with law enforcement agencies, ISPs and content providers (for hotlines)	T3	R	C
D9.1	Helpline progress report including Help line operating guidelines and Helpline training module[5]	T6	R	C
D9.2	Helpline progress reports[5]	T12, T18, T24	R	C

1 Deliverable numbers in order of due dates. The numbers should indicate which work package they relate to, e.g. D2.1 for the first deliverable of work package 2.

2 Due dates for transmitting deliverables to the Commission. T0 indicating the start of the project and all other dates being relative to this date.

3 Code for nature of deliverables:
R = Report
S = Software/Prototype/Demonstrator
O = Other

4 Codes for dissemination level:
P = Public
C = Confidential, only for members of the consortium (plus Commission services and project reviewers) and, except for cost statements, for the network coordinator and other members of the network

5. Relevant only to participants who include Work Package 9 - Helpline

Reports should be delivered in English on paper and in electronic form. Public reports should be in a format suitable for publication. Software deliverables (modules, web sites, prototypes, demonstrators) should be delivered either on Internet or CD-ROM.

European added value and network contribution (maximum 1 page)

The Knowledge Agency Society (UMIC), as PSI project coordinator will establish the bridge with European networks INHOPE and INSAFE, acting when necessary in international settings. With the project implementation the Portuguese citizens will be able to report illegal content [pornography, xenophobia, hate speech, racism, (…)] to the hotline and to report harmful content to the awareness node. The actions implemented by the consortium within this project will be mostly the result from the efforts held with our partners and networks in the field, nearby schools, teachers, students, parents, governmental and civil society entities.

Through FCCN, the consortium can have a unique role in providing guidance in network security, due to its continued experience as part of the Trans-European Research and Education Network. FCCN is, in collaboration with other operators of National Research and Education Networks across Europe, actively involved in developing security services and applications for a new backbone for this European network – GEANT2. FCCN's CERT.PT is also involved in European *fora*, mainly TERENA's TF-CSIRT – a Task Force for Collaboration of Computer Security Incident Response Teams and, therefore, it is permanently aware of the main issues affecting wide area networks in the European space and it works together with these agencies to promote awareness in security related fields. FCCN also sponsored the creation of a national forum for ISPs regarding security issues and has been an element of liaison between this group and the European abuse teams forum ECOAT. This work can be complemented and will benefit by the inclusion of FCCN as a contributing partner within the Awareness Node actions.

Through Microsoft, the consortium will be able to share the project and promote the usage and replication of best practices all over the European countries where the company has a presence. Microsoft will bring to the discussion of the local consortium, projects that were implemented with a huge success in Italy, Finland and UK. It will allow the consortium to work closer with Austria, Germany and the UK where Microsoft is also associated in similar consortia. The idea is to create a strong network of collaboration and best practices sharing.

Through DGIDC/CRIE, the consortium can contribute to the European network by sharing the awareness tools and methods developed within this project as well as their results, and integrating them with the broader mission of our task force: to foster learning through the added value of ICT both for educational as well as citizenship and training purposes, taking into account perceived safety risks on their use.

.