



TRAINING MANUAL

**SAFER Internet
CYPRUS HELPLINE**



2009

CyberEthics Program Director	Dr. Yiannis Laouris
CyberEthics Helpline Directors	Mrs. Ninneta Kazantzi Mrs. Skevi Koukouma
Project coordinator(s)	Mrs. Georgina Shitta Dr. Aysu Arsoy
Author	Mr. Lawrence Kalogreades
Co-author	Mrs. Elena Aristodemou
Editors	Mrs. Marta Wojtas Dr. Yiannis Laouris
Scientific Team	Dr. Yiannis Laouris, Dr. Aysu Arsoy, Mrs. Tatjana Taraszow, Mrs. Elena Aristodemou, Mrs. Georgina Shitta, Mrs. Yiola Papadopoulou.

This Training Manual was prepared by Future Worlds Center (legally registered as Cyprus Neuroscience & Technology Institute) in the context of the project:

CyberEthicsGII

Grant agreement Number: SIP-2008-CNH-143802, funded by the Information Society and Media, Directorate General.

http://ec.europa.eu/information_society/activities/sip/projects/awareness/cyprus/index_en.htm
www.CyberEthics.info



CyberEthics aims to raise awareness in parents, educators and children on issues concerning Internet safety, ethical use of mobile phones and new online technologies in general. Priority issues include child pornography, racism, gender discrimination, giving out personal information and inappropriate use of people's images either on mobile phones or the web.



Co-funded by the Safer Internet Plus Program of the European Commission.

All Rights Reserved. Copyright Future Worlds Center (legally registered as Cyprus Neuroscience & Technology Institute) Nicosia 2009.

Cyberethics-Helpline; Training Manual
ISBN XXXXXXXX

<u>Executive summary.....</u>	<u>6</u>
<u>Context concerning the creation of the Helpline.....</u>	<u>6</u>
<u>Background of the Safer Internet Helpline.....</u>	<u>7</u>
<u>General overview of the training process.....</u>	<u>7</u>
<u>1. What is this training about?.....</u>	<u>7</u>
<u>2. Who can participate in this training?.....</u>	<u>7</u>
<u>3. What are the phases and modules of the training?.....</u>	<u>7</u>
<u>4. Training guidelines.....</u>	<u>7</u>
<u>What are the target groups of the Helpline?.....</u>	<u>8</u>
<u>When children contact the Helpline they may be experiencing:.....</u>	<u>8</u>
<u>Their requests may be to:.....</u>	<u>9</u>
<u>Forms of Internet abuse:.....</u>	<u>9</u>
<u>Cyber-bullying.....</u>	<u>9</u>
<u>Grooming.....</u>	<u>10</u>
<u>Hacking.....</u>	<u>11</u>
<u>Internet addiction.....</u>	<u>11</u>
<u>Inappropriate content.....</u>	<u>11</u>
<u>How to answer a call:.....</u>	<u>12</u>
<u>Calls are divided into two types:.....</u>	<u>12</u>
<u>When dealing with an eligible call, counselors are expected to:.....</u>	<u>13</u>
<u>What information should be documented?.....</u>	<u>13</u>
<u>It is vital that counselors:.....</u>	<u>13</u>
<u>Counselors should have the psychological skills necessary to:.....</u>	<u>13</u>
<u>Counselors should also understand the legal elements of a call:.....</u>	<u>14</u>
<u>An up-to-date knowledge of Internet safety in Cyprus is also vital:.....</u>	<u>14</u>
<u>The most important policy however is that of.....</u>	<u>14</u>
<u>Anonymity.....</u>	<u>14</u>
<u>Eligible phone calls are handled in the following manner:.....</u>	<u>15</u>
<u>Case assesment</u>	<u>15</u>
<u>Consultation</u>	<u>15</u>
<u>Legal advice.....</u>	<u>15</u>
<u>Providing psychological support.....</u>	<u>15</u>
<u>Cooperation with the SafenetCY Hotline.....</u>	<u>15</u>
<u>How to provide effective and therapeutic communication:.....</u>	<u>15</u>
<u>Reflective (or active) listening.....</u>	<u>15</u>
<u>Matching speech patterns.....</u>	<u>17</u>
<u>Paraphrasing.....</u>	<u>17</u>

<u>Asking questions.....</u>	<u>18</u>
<u>Data questions.....</u>	<u>18</u>
<u>Questions about feelings and values.....</u>	<u>18</u>
<u>Open and closed questions.....</u>	<u>18</u>
<u>Matching verbal styles.....</u>	<u>19</u>
<u>Matching breathing patterns.....</u>	<u>19</u>
<u>Examples of advice to be given when cyber-bullying is reported by a minor:.....</u>	<u>19</u>
<u>Examples of advice to be given when a case of grooming is reported by a minor:.....</u>	<u>20</u>
<u>Examples of advice to be given when a parent or professional reports an incident:....</u>	<u>21</u>
<u>Examples of advice to be given when illegal content is reported by a minor:.....</u>	<u>21</u>
<u>Where to direct callers in order to report a crime:.....</u>	<u>22</u>
<u>The SafernetCY Hotline:.....</u>	<u>22</u>
<u>The Cyprus Police Cyber Crime Unit:.....</u>	<u>22</u>
<u>How to submit a report to our Safer Internet Hotline:.....</u>	<u>22</u>
<u>How to report a crime to the Cyprus Police Cyber Crime Unit:.....</u>	<u>24</u>
<u>How to properly record evidence of illegal or inappropriate content or communications:.....</u>	<u>24</u>
<u>The monthly Helpline operator meeting:.....</u>	<u>25</u>
<u>Social Networking Websites.....</u>	<u>29</u>
<u>Appendix I.....</u>	<u>32</u>
<u>How do you react if a caller asks for a specific person?.....</u>	<u>32</u>
<u>How do you react if a caller wants to know more about you?.....</u>	<u>32</u>
<u>What is the course of action if repeated test calls are being made?.....</u>	<u>32</u>
<u>What to do if you decide that a caller requires on-going psychological support:.....</u>	<u>33</u>
<u>What should be the course of action if you determine that a crime has occurred?.....</u>	<u>33</u>
<u>Are there any cases where it is necessary to breach confidentiality?.....</u>	<u>33</u>
<u>Where can I find out more about the legislation surrounding Internet use and crimes so that I can have an idea of what constitutes an Internet-crime?.....</u>	<u>34</u>
<u>Appendix II.....</u>	<u>35</u>
<u>Appendix III.....</u>	<u>42</u>
<u>Appendix IV.....</u>	<u>43</u>
<u>Ccleaner – A freeware application which cleans your hard-drive and registry of any files which are not part of your system but may have been placed there by malicious software.....</u>	<u>43</u>
<u>Spybot Seek & Destroy – A free application which detects any malicious software or spyware which may be lurking on your harddrive or in your memory.....</u>	<u>43</u>
<u>Avast! Antivirus – A freeware antivirus package.....</u>	<u>43</u>
<u>Comodo – A freeware firewall application.....</u>	<u>43</u>
<u>We-Blocker Safe Families software – A free Internet filtering and parental control application.....</u>	<u>43</u>

<u>Appendix V.....</u>	<u>44</u>
<u>Appendix VI.....</u>	<u>47</u>
<u>Cyprus.....</u>	<u>47</u>
<u>Europe.....</u>	<u>48</u>
<u>International.....</u>	<u>50</u>
<u>Appendix VII.....</u>	<u>52</u>

Executive summary

This training manual has been prepared by the CyberEthics team to serve the needs of training psychologists who wish to work for the Helpline. The goal of this manual is to provide new trainees with the necessary information in order to work at the Safer Internet Helpline.

The material covers the procedures and background knowledge required for the operation of a Safer Internet Helpline for Children. Some of the practical examples were derived from Poland's Safer Internet Helpline (helpline.org.pl). The manual was created in such a way as to stimulate the trainees to become more deeply involved in the subject matter. Due to the ever changing nature of the Internet and mobile communication technologies as a whole, the information herein will be under frequent revision. Thus, the trainees will have the two-fold task of assimilating the material, but also cross-checking it in order to stay up-to-date.

In line with this policy, the content has been formulated in a manner which can provide the necessary initial guidance and impetus, which is required for individuals with a background in psychology or pedagogy to become accustomed with the context of cyberspace, raise questions, and extend their knowledge further.

Thus, the manual is enriched with links to external sources, as well as details of journal articles, which serve to provide even more information and help promote further reading on the subject.

Context concerning the creation of the Helpline

The European Commission has reported that due to the wide use of Internet technologies and the lack of adequate monitoring and legislative processes, children may place themselves in a high risk situation when encountering dangerous or illicit content and may experience fear, intimidation and bullying.

The Safer Internet Plus program funds Internet Safety Helplines across Europe.

The Safer Internet Helpline for Children aims to provide the public and children in particular with the means to talk anonymously to a professional who may support them psychologically when dealing with complex Internet risks while also assisting in the report of illegal webpages, activities, and also technical and software issues, or even advice on which websites to avoid.

More information can be derived from the website of the project at www.cyberethics.info.

Background of the Safer Internet Helpline

The Cyprus Neuroscience and Technology Institute (CNTI) launched an Awareness Node for Safer Internet in 2006 and a Hotline in 2007. Since 01/09/2008, the CNTI is coordinating the operation of a combined Node which includes an Awareness Node, a Hotline, and a Helpline.

The Safer Internet Helpline has been the result of the collective efforts of the Pancyprian Coordinating Committee for the Protection and Welfare of Children (PCCPWC) and CNTI. The launch of the Safer Internet Helpline for Children took place in January 2009. A three day training, which took place between the 22nd and 24th of January prepared the first personnel for their tasks.

General overview of the training process

1. What is this training about?

The training aims to prepare experts to serve as counselors for the Helpline. It provides logistical, scientific and technical knowledge and skills required for the job.

2. Who can participate in this training?

Participants are people who wish to work as volunteers or counselors for the helpline.

The counselors are expected to have a background in psychology, counseling, pedagogy, or a similar discipline which places an emphasis on developing communication skills.

The nature of the Helpline naturally means that the counselors must be familiar with new media, the use of popular operating systems and must stay up-to-date with the sorts of games, communication applications and social networking websites that are popular with children and adolescents.

3. What are the phases and modules of the training?

This document serves as the guideline throughout the training. However it does not contain all the information needed in order to perform flawlessly as a counselor. Potential trainees need to study the additional materials, which are suggested in this manual, view the training videos and acquaint themselves with the wide spectrum of new technologies, and attend as many external training workshops as possible which are related to providing children with psychological support.

4. Training guidelines

The counselors of the Safer Internet Helpline for Children are expected to provide:

- Counseling in the field of children and youth's safety on the Internet.
- Providing help in cases or suspected or confirmed threats to children on the

Web.

- Interventions in cases of child abuse via the Internet.
- Improving the knowledge and skills of professionals who work in fields related to children's safety on the Web.
- Counseling in the field of prevention of Internet-related child abuse.

What are the target groups of the Helpline?

Our service encourages children to contact us when:

- bullied, threatened or blackmailed.
- they receive crude messages.
- someone on a chat or communicator asks them embarrassing questions, demands their photos, or insists on a face-to-face meeting.
- they receive or are shown inappropriate content, such as pornography or violence.

We also encourage parents to contact us when:

- they don't know how to talk with their children about Internet safety.
- they are concerned about their children's on-line "friends" and activities on the Web.
- their children have been exposed to dangerous content.

Professionals who encounter such cases are also encouraged to contact us when:

- they come across public content which they recognize as illicit or hazardous in the context of webpages used by children and adolescents.
- children or their parents ask them for help in resolving problems related to Internet safety.

When children contact the Helpline they may be experiencing:

- Fear
- Anxiety
- Confusion
- Powerlessness
- Distrust
- Sadness
- Shame
- Disappointment

Their requests may be to:

- immediately cancel published content.
- block contact with a person on the Internet.
- feel comfortable about their problem and lose track of time.
- do something to improve the situation.
- to offer help.

In general terms, the child is experiencing a **crisis**. This could be due to a variety of different forms of abuse, some of which are described below.

Forms of Internet abuse:

Cyber-bullying

...is the term used to define various forms of psychological abuse, akin to conventional bullying, communicated via the Internet. For example:

- Repeated mockery of a person's nick.
- Sending obscene short text messages from the Internet.
- Sending obscene and offensive content and intimidating children via messenger applications.
- Obscene content conveyed during chats.
- Ridiculing a child by creating profile or blog copies with false or humiliating information.
- Sending threats through communicators.
- Publishing private video footage or photographs of an individual without their consent.

Cyber-bullying usually occurs in the context of instant messenger applications such as AIM, Skype or MSN Messenger.

However it may take even great dimensions by becoming even more public, when it takes place in the context of public blogs or social networking sites such as MySpace, FaceBook, hi5, or even media hosting sites such as YouTube.

Cellular phone tools such as SMS or photographic and video footage captured using a cellular phone may also be used as a means of cyber-bullying.

Grooming

...is the preparation and psychological manipulation of a child with the intent of sexual exploitation.

- The first step of grooming is to gain the trust of a child, with the groomer presenting his/her actions as beneficial for the child.
- This may occur in the context of private communication via messenger programs.
- Other times it may occur in forums or Social Networking Sites. The individual who is initiating the grooming may have some sort of stature or position in the website which makes it easier to form a relationship with a child.
- The goal of these interactions is to arrange a meeting with the child, or to manipulate the child so as to obtain child pornography.
- Grooming can be the cause of psychological harm due to the psychomanipulation and seduction used by the groomer. It also creates a harmful model of child-adult relationships.

Grooming is a very serious offense that requires immediate attention. It may require direct cooperation with the police, motivating the child to report the offense and working with the victim's family.

- Signals of grooming may be:
 - Showing interest or preference for a particular child or expressing a willingness to meet in person.
 - Sending pornographic images, videos or links to a child.
 - Leading a conversation towards sexual or age-inappropriate topics.
 - Asking a child to share personal or intimate images.
 - Giving benefits or allowing a child to get away with inappropriate behavior.
 - Sharing problems or issues with a child which are not age-appropriate.

Hacking

...is the term used to describe an attempt to digitally break into someone's computer and access their files and personal information, manipulate their operating system, software or hardware, and generally to gain control of material on someone else's computer without their consent or knowledge.

- This can be quite distressing because it implies that someone may have accessed personal files, accounts and information.
- This may be the beginning of a variety of serious issues, with the perpetrator going on to perform a range of activities, such as fraud or publicly disseminating personal information.
- In other cases, the hacker's activities may cause the deletion of important files or damage to the computer, which may also cause significant distress.

Phishing

...is the term used to describe an attempt by a party to extract another person's security passwords, personal information, banking details, user-names and other such sensitive information in order to commit fraud or extortion.

- Phishing emails are usually disguised as a legitimate enterprise or call for help, offering a large bulk of information which is supposed to convince the receiver that the subject of the email is true.
- For example, phishing emails may describe how the receiver has won the lottery in another country or has inherited a large amount of money from a distant relative. The emails are usually portrayed as coming from a national authority or legal representative, who asks for a down-payment to be made in order for the total sum of money to be transferred to the receiver's bank-account.
- Unsuspectingly, the receiver shares his/her banking details and personal information, only to find out that all the money in their bank-account has been withdrawn. The fact that the receiver gave his/her consent and sensitive details makes the matter very complicated from a legal standpoint.

Internet addiction

...is the excessive use of the computer that interferes with daily life. Although this may seem ambiguous, there are cases where children and teens spend numerous hours on end playing computer games, chatting, or surfing the net while forgetting their responsibilities or even to eat.

From a behavioral standpoint, it may be considered a compulsive behavior, clinically defined as a behavior which is performed not because it is enjoyable but because the individual feels that he or she has to.

Inappropriate content

...is a label for any sort of Internet content, whether verbal, visual or auidial which may be illicit, dangerous, or age-inappropriate and yet publicly available.

- Due to the size and scope of the Internet, it caters to a huge variety of interests and subjects.
- Without the proper guidance or filtering software, children may purposefully or even by accident access pages with content which may cause significant distress.
- Such content may be violent, pornographic, racist, or insulting.
- Watching such content may cause mess in inner world of a child, cause feelings of anxiety and danger. In the case of watching pornography, it may also distort psycho-sexual development, encourage a child to actions against himself or others, or even encourage a child to meet people who can hurt him/her

Some times children may contact the line simply because they are seeking general information about the Internet or how to perform certain tasks.

They may wish to:

- learn how to install filters or firewalls.
- find out which websites contain appropriate content and which websites to avoid.
- ask for advice relating to the Internet.

Our website, www.cyberethics.info is a great resource for children (and parents) with such questions!

How to answer a call:

Counselors are expected to answer the phone with a simple and polite “Internet Safety Helpline, how may I help you?”

It is important that this is said in a steady, affirming tone of voice each time that the phone is picked up. Counselors must maintain their tone steady and consistent each time they answer the phone in order to not dissuade callers from talking.

An outline of communication skills will be provided in a seperate section.

Calls are divided into two types:

- Eligible
- Test calls
 - Joke calls, pranks.
 - Mistakes or wrong numbers.
 - Dead.

All calls are considered to be eligible by default and for this reason they must be treated as real calls for help. The children calling may still be trying to find the courage to talk or may be trying to test the Helpline counselors in order to see if they are trust worthy and for

this reason they may hang-up or make jokes.

It is important that the counselors keep this in mind and remain calm and professional in such situations.

When dealing with an eligible call, counselors are expected to:

- Verify the reported case.
- Provide information and support.
- Undertake intervention, if necessary.
- Refer the case to another institution (such as the police) if warranted.
- Monitor each accepted case.
- Document reports.
- Seek consultation in the case of insufficient knowledge or skills.

What information should be documented?

Counselors should complete each cell of the call database in line with the call.

First, it should be noted if the call was eligible or a test call. In the case of a test call, the type should be noted along with what was said by the caller.

If the call was eligible, the reason for the call should first be noted. Then whether a crime was reported and if so what, along with what sort of advice or action the counselor offered. If the caller was advised to contact another service or institution, its name should be noted as well as the reason. It should also be noted if the SafenetCy Hotline was contacted in order to make a report.

Finally a short description of the conversation should be noted.

It is vital that counselors:

- are familiar with Internet terminology.
- understand the portals that are used by children and youngsters.
- have the necessary skills to contact a website administrator.
- know how to operate on-line applications or communicators.
- know the general rules of web functioning.
- know how to seize evidence (I.e. print screen, recording)
- understand how to use and explain the use of filtering software and firewalls.

Counselors should have the psychological skills necessary to:

- initiate contact with calling person.

- maintain the conversation.
- figure out the problem.
- give support.
- motivate clients to accept psychological help.
- talk to children's caregivers.

Counselors should also understand the legal elements of a call:

- Evaluation of evidence.
- Legal aspects of offenses against children on the Internet.
- Rights and obligations of Internet service providers.
- Children's legal liability on the Web.

An up-to-date knowledge of Internet safety in Cyprus is also vital:

- Knowledge of issues related to children's safety on the Internet (theory, epidemiology, legal regulations, preventive measures).
 - Knowledge of up-to-date national and international reports on the problem.
 - Knowledge of relevant institutions.

The most important policy however is that of...

Anonymity

It is extremely important that counselors do not in any way directly ask for or maneuver a telephone conversation in a manner that will require the caller to share details regarding their identity.

This compromises the entire phone call because it breaches the main reason why children call helplines in the first place – anonymity.

In the case where anonymity is impossible because the counselor has been provided with links to someone's personal profile, it is important to explain to the caller that the helpline guarantees that all the information provided shall and will remain confidential.

Eligible phone calls are handled in the following manner:

Case assesment

- What is a nature of the problem? Who needs what kind of help?

Consultation

- Providing information on safety rules.
- Giving advice on how to seize the evidence.

Legal advice

- Assess if the report describes behaviors constituting a criminal offense and if so, what offense has been committed.
- Information about legal action to be taken.
- Providing help in writing formal documents, such as a notice of an offense.

Providing psychological support.

Cooperation with the SafenetCY Hotline.

How to provide effective and therapeutic communication:

Once the conversation has begun, there are a few communication skills which can be used in order to establish and improve the rapport (the feeling of mutual trust and respect) between the caller and the operator. These skills are especially important if the caller requires emotional support.

The goal is always to be attending and give the impression of showing concern and understanding. It is easy to miss this point due to the fact that the entire interaction is taking place over the phone. Thus extra emphasis must be made in order to create a sense of empathy.

Reflective (or active) listening

...is the process where the listener (in this case the operator) tries to clarify and restate what is being said. This allows the listener to better understand the situation and the caller as an individual, it can help the caller clarify his or her own thoughts, and it also provides the caller with the feeling that the listener is willing to offer acceptance and support.

It can briefly be described as listening for meaning.

Fisher (1981) effectively outlined some of the principles of reflective listening:

- More listening than talking
- Responding to what is personal rather than to what is impersonal, distant, or abstract.

- Restating and clarifying what the other has said, not asking questions or telling what the listener feels, believes, or wants.
- Trying to understand the feelings contained in what the other is saying, not just the facts or ideas.
- Working to develop the best possible sense of the other's frame of reference while avoiding the temptation to respond from the listener's frame of reference.
- Responding with acceptance and empathy, not with indifference, cold objectivity, or fake concern.

It is important to maintain the conversation on the person and the situation without deviating to more general subjects. For instance, in a case of cyber-bullying it is more effective to respond "I understand your concern, they should not have uploaded that photograph" rather than "Maybe no-one will see the photograph because that social networking site is not popular".

It is important to place as much focus on the feelings of the caller as on the content of the conversation. This allows for a feeling of deeper understanding to develop. Also, the caller may actually be in more need of support in order to deal with the emotions caused by the problem, rather than the actual problem itself.

The emotions of the caller can be detected in their tone of voice, their vocabulary and the syntax that they use.

Fisher (1981) outlined some things to avoid in regards to reflective listening:

- *Stereotyped Reactions*. Constantly repeating a phrase like "you feel that ..." or "you're saying that ..."
- *Pretending Understanding*. If you get lost, say "sorry, I didn't get that. What are you saying?".
- *Overreaching*. Ascribing meanings that go far beyond what the other has expressed, such as by giving psychological explanations or by stating interpretations that the other considers to be exaggerated or otherwise inaccurate.
- *Under-reaching*. Repeatedly missing the feelings that the other conveys or making responses that understate them.
- *Long-windedness*, Giving very long or complex responses. These emphasize the listener's massive effort to understand more than they clarify the other person's point of view. Short, simple responses are more effective.

- *Violating the other person's expectations.* Giving reflective responses when they are clearly not appropriate to the situation. For example, if the other person asks a direct question and obviously expects an answer, simply answering the question is often best. In other words, if someone says: "what time is it?" you don't usually say "You're feeling concern about the time".

Matching speech patterns

...is the process of emulating the speed and syntax of the caller's speech. This allows the operator to sound more familiar and relevant to the caller, which helps improve rapport.

Paraphrasing

...is useful in order to portray that you are engaged as a listener and also to encourage the speaker to continue. It also allows for you to clarify if you are sure that you understand what is being said. For example, if a caller says "I was given this link by a friend and I typed it in and when the website appeared it was full of pornographic content and I got worried because someone might find out and I didn't like it anyway", you could paraphrase briefly by saying "So when you saw the content you became anxious", eliciting the reply "Yes, so I..." - thus encouraging the speaker to continue with more detail.

Asking questions

Avoid asking too many questions, especially too early in the conversation. This is likely to dissuade the caller from wanting to talk freely. Do not stick to simply asking about the subject – inquire about the caller's feelings and emotions.

Data questions

If you want a clear and concise answer, don't ask “why?” because it usually causes the other person to become defensive and apologetic. Instead ask “how?”, “what?”, “when?”. For instance, if a child says “They all behave differently around me because they all hate me”, don't ask “why?”, instead ask “how do they behave?” or “what do they do?”. After the child explains that, you can ask “what do you do if you like people?” and lead the conversation to more positive and confident ground.

Questions about feelings and values

It is important to make questions that appear empathic and understanding. Ask “how do you feel about this?” or “what do you prefer?” or “what did you feel?”.

If possible, lead the caller to not just use their emotions but also their sense of logic in order to begin putting things into perspective and assume control. For instance, you can ask “what is the worst situation that you can imagine?” or “what would you prefer to happen?”. This opens up options for actual action to be taken.

Open and closed questions

Questions have the ability to control a situation. Closed questions are straight to the point. They simply ask for information and may even be answered with a single word or have a single possible answer.. They are controlling because they lead the situation, which may make the caller feel like they are being controlled rather than supported. An example of a closed question is “How many times did he try to call you?”.

Open questions allow a greater possibility of freedom in the response, giving the caller the chance to think more about an issue and perhaps take a position. An example is “How did you feel when he tried to call you?”

Good questions:

- are short
- are delivered one at a time.
- do not need explain
- are followed by some time that allows for an answer
- should not be answered by the person asking them
- should not appear like an interrogation

Matching verbal styles

...is important in order to improve the sense of security, familiarity and effective communication between the caller and the operator. If the operator uses the same words as the caller to describe something, for instance "P.C" rather than "computer" or uses their expressions, such as emulating a caller's habit of saying "cool" or "OK" at the end of each sentence, helps create a feeling of mutual understanding between the two individuals.

This is very important because if the callers are children, their vocabulary and possibly their communicative abilities will not be the same as those of the operator. For this reason, the operator must try and talk in a way that is understandable and familiar to the child.

Matching breathing patterns

...is method of building unconscious emotional rapport with another individual. Because a telephone conversation lacks visual information, paying attention to a caller's breathing rate is a helpful way of understanding their emotional state.

A useful way of utilizing this technique is to have the operator match the caller's breathing rate and then subtly slow it down. If the rapport is strong, the caller will follow the operator's lead and also slow down his or her breathing rate, effectively helping the caller relax and calm down.

Examples of advice to be given when cyber-bullying is reported by a minor:

- **Do not reply** to any communication, whether messages, calls, or emails that are made with the intent to disturb you. This simply encourages whoever is bullying you to continue.
- **Do not delete the messages:** if you identify a message as material that is meant to bully, intimidate or harass you, keep it in order to provide the authorities with proof of the incident. It is not necessary that you open the message and read it.

The operators however should open such documents in order to establish the nature of the reported content.

- **Notify** people who can do something about the incident. You can make a report to our **Hotline** about the material or communication which has bothered you. You do not have to put up with it! If you believe that someone's on-line content or activities are illegal, you can talk about it with us or your parents, or whomever you feel comfortable with. If you feel that it is very serious, we can arrange to notify the authorities together. This can include both the website's administration and our Hotline, but also the police.
- **Block the sender:** Don't put up with whoever is harassing you. Block them.
- **Talk to someone you trust:** Talking about the issue with your parents, friends, teachers, and people you trust is a good way to begin dealing with harassment.
- **Cyberspace is public space.** It often seems that cyberspace is separate from

public life, but this is far from the truth. Know what you post, know your rights, and know your responsibilities. Be respectful and stay in control.

- **If the caller is significantly distressed:** advise the caller to arrange a meeting with a counselor or psychologist in order to receive expert help. If the caller is under-aged, advise the child to talk to his or her parents in order to organize something with their consent.

Examples of advice to be given when a case of grooming is reported by a minor:

Grooming is committed when an adult intentionally initiates contact with a minor in order to arrange a meeting, with the intent of committing a sexual offense.

Harm does not necessarily have to occur to the minor for the incident to be deemed an offense.

Examples of advice to be given:

- **Do not reply** to any further communication with the individual you suspect is grooming you.
- **Do not delete the messages:** if you identify a message as material that is meant to manipulate you into a personal meeting, keep it in order to provide the authorities with proof of the incident.
- **Notify the authorities:** Grooming is a criminal offense and the police can take immediate action. If you agree, we can explain how to notify the webmasters, Internet Service Providers, the police and our Hotline that a user is attempting to groom you.
- **Block the sender:** Don't tolerate or encourage any further communication with the groomer. If you are being black-mailed, explain what has been said and we can think of a way to provide the authorities with enough time in order to track the person down.
- **Talk to someone you trust:** Talking about the issue with your parents, friends, teachers, and people you trust is a good way to begin dealing with grooming.
- **Cyberspace is public space:** Be rational when you talk with strangers in cyberspace. Do not immediately trust people, or given them your personal details, photos, or agree to initiate a meeting. If you choose to meet them anyway, make sure that you tell your parents about your plan. If you meet, do so in a public space where there are plenty of people around so that you may remain in control of the situation. Arrange for your friends to go to the meeting with you – do not go alone.
- **If the caller is significantly distressed:** advise the caller to arrange a meeting with a counselor or psychologist in order to receive expert help. If the caller is under-aged, advise the child to talk to his or her parents in order to organize something with their consent.

Examples of advice to be given when a parent or professional reports an incident:

- **Do not delete the messages or content:** if you identify a message or content on a minor's computer or account as material that is illegal or inappropriate, keep it in order to provide the authorities with proof of the incident.
- **Discuss the possibility of notifying the authorities:** encourage parents and professionals to talk with the minor, offer support and discuss with them the possibility that the authorities should be informed about the incident.
- **Encourage the minor to talk about the incident:** Talking with the minor about the incident can provide significant relief and confidence in order to begin dealing with the issue.
- **Install firewalls and filters:** software exists that can automatically block access to certain content and also block outsiders from accessing your computer. Recommendations and links to quality free-ware as well as commercial software should be given as well as any guidance as to how to install and use it.
- **Cyberspace is public space:** parents and caretakers must recognize this. Cyberspace is littered with as much crude, inappropriate or sexual content as our cities. It is a good idea to protect minors from such content by installing filters, firewalls, and providing minors with the proper guidance, advice and skills in order to recognize hazardous situations and avoid them.
- **If the incident has caused significant distress to anyone involved:** advise the caller to arrange a meeting with a counselor or psychologist in order to obtain expert help. If the caller is under-aged, advise the child to talk to his or her parents in order to organize something with their consent.

Examples of advice to be given when illegal content is reported by a minor:

Illegal or inappropriate content may be in the form of videos, images, text, or audio which is evidence of a crime (I.e child-pornography, violence, torture, etc.) or material that is inappropriate for the age-group of the users of the website.

- **Do not reply** to any further communication with the individual who sent you the material or the link.
- **Do not delete the content:** if you received the content was unwillingly forwarded to you and you recognize it as illegal or inappropriate, do not delete it. Simply close it or do not open it if possible, and provide the authorities with a link or a copy of the material.
- **Notify the authorities:** You can notify the web-masters and our Hotline if you identify content as inappropriate or illegal. Our Hotline will make all the necessary reports to the authorities.
- **Block the sender:** Don't tolerate or encourage any further communication with whoever sent you the content.

- **Talk to someone you trust:** Talking about the issue with your parents, friends, teachers, and people you trust is a good way to begin dealing with any distress caused by viewing the content.
- **Cyberspace is public space:** Be rational when you talk with strangers in cyberspace and do not access areas of cyberspace that appear to be dangerous or contain signs of illegal activities.
- **If the caller is significantly distressed:** advise the caller to arrange a meeting with a counselor or psychologist in order to receive expert help. If the caller is under-aged, advise the child to talk to his or her parents in order to organize something with their consent.

Where to direct callers in order to report a crime:

The SafenetCY Hotline:

SafenetCY is the Hotline that promotes the safe use of Internet in Cyprus. It serves the needs of all people that live on the island (i.e., also Turkish Cypriots and other minorities) and addresses issues of child pornography, child erotica, child nudism, child grooming activities, child trafficking, child sex tourism, but also racism (currently on the rise in Cyprus), gender discrimination and inappropriate use of peoples' images.

It operates as a combined Awareness Node and a Hotline under the name CyberEthics. The project engages actors from the government and the civil society, thus contributing towards the eradication of cyber crime through informed actions of European citizens and public institutions that aim to change behaviors, mentality and attitudes, giving special emphasis to rural and less developed areas of the country.

The Cyprus Police Cyber Crime Unit:

The Unit was created in 2007 in order to combat the increasing phenomenon of Internet related crimes and to also protect the increasing number of young Internet users in Cyprus.

The Unit investigates offenses as outlined in the Cyber-crime Law of 2004, 22(III)/2004.

How to submit a report to our Safer Internet Hotline:

You can select one of the following ways to submit your report. On-line reports are preferable since they are accepted automatically.

Online: You could fill in the on-line reporting form at:

(<http://www.cyberethics.info/cyethics2/page.php?pageID=56&mpath=/72/81>)

Telephone: 22 67 47 47

Regular mail: 5 Promitheos Str., 5th floor, office 9, 1065 Nicosia.

In order to make the processing of your report as effective as possible you are required to provide us with specific information depending on the location and type of illegal content you encountered.

For each different type of report please be prepared to provide us with the corresponding information:

- **Website:** Website address (URL), day and time you looked at the content, type of content, a free text description of the content.
- **Newsgroup:** Name of newsgroup, message ID, message sender, message subject, date of the message, type of message content, a free text description of the content.

Anonymity

You could always choose to keep your anonymity by not providing contact information. Making an on-line report does not automatically implies that you lose your anonymity. We register only the information you give to the on-line form. We do not register any other information, not even the IP address of the machine you use to submit your report.

Contact Information

If you wish to be notified about the outcome of your report you should provide us with sufficient contact information:

First Name, last Name, address, email, etc.

The steps SafenetCY follows, in order to process reports it receives, are:

- **Verification:** First, SafenetCY performs a typical verification of the reported content. If, for example, the report complains about a website, SafenetCY verifies that the address (URL) given exists and that its content is possibly illegal.
- **Tracing the source:** Then, an attempt is made, using technical means, to trace the country where the reported content originates from.
- **Cyprus Police notification:** SafenetCY forwards all reports, regardless of the originating country of the reported content, to the Cyprus Police.
- **Foreign hotline notification:** If the reported content originates from abroad, the report is also forwarded to a hotline in the country of origin (if one exists).
- **Feedback:** If the user that made the report has provided any personal details, then SafenetCY informs him of the actions taken based on his report.

How to report a crime to the Cyprus Police Cyber Crime Unit:

Callers can be given the following phone numbers, fax and email address in order to contact the Unit as they see fit, depending on the degree of anonymity they prefer to maintain.

Phone # 22-808200, 22-808456, 22-607250

FAX # +22-808465

(cybercrime@police.gov.cy)

An alternative is to dial 112 or 1460 and ask for the Cyber Crime unit.

How to properly record evidence of illegal or inappropriate content or communications:

When it is decided that it is necessary to collect evidence in order to assist in the proper report of a file, crime or complaint, the counselor should attempt to guide the caller in taking all the necessary actions.

In the case of a web-page containing illegal or inappropriate content, the initial step is to ask the caller to provide the name of the website where the content is located and if possible a URL link to the specific page where the content was posted.

The counselor must forward the URL as well as a description of the content to the Hotline, which will take the responsibility of reporting it to the authorities.

If a serious offense has occurred, it may be necessary to record visual or audio material in order to be used as evidence. This should be done to prevent the loss of evidence if the website removes the content before legal action takes place.

In the case where child pornography is reported, do not in any case open it on the Helpline's computers because this makes you and the organization an accomplice in the crime. In such cases simply report the link or file immediately to the Hotline.

Recording such evidence is also important if the abuse is taking place in a chat-room. Because the conversations are private and usually not saved on the computer's hard-drive, it is important to record a series of images which document the entire conversation.

Image, audio and video capture are explained below.

The monthly Helpline operator meeting:

Each month, on the 4th Monday, a meeting will be scheduled in order for the entire group to meet and discuss various issues while in the presence of a professional external counselor. The purposes of the monthly counseling meetings are multiple:

- For the coordinator to brief the operators of any news, changes in procedure, or matters of discussion.
- For each operator to discuss the calls they received and how these calls raised new issues or provided good examples of a particular case.
- To provide each other with feedback regarding their general conduct, successes and failures throughout the week.
- To provide each other with support on the occasion where a particular case caused a significant amount of stress.

- **How to capture images:**

- **The Print-Screen (PrtSc) function:**

Windows permits the user to capture screen shots of their operating system while it is in action. Essentially, whatever is being displayed at that moment will be copied onto the clipboard and can then be pasted into a word-processing or image-processing program.

This allows the user to record images of chat-room activities, websites, or visual media while they are in action.

Helpline counselors should encourage their callers to use the Print-Screen function in order to record visual evidence if a criminal offense or complaint needs to be made to an authority.

- **Performing the Print-Screen function:**

- Simply locate the Function (fn) button (usually located between the Control, Windows, and Alt buttons on the bottom line of keys on the keyboard) and keep it pressed.
- Then, while the Function key is being held, press the Print-Screen button, which is usually located in the top-right portion of the keyboard. This saves the monitor's output into the clipboard.

Note: On some systems, it is not necessary to use the Function key.

- Then open a word-processing program (such as Microsoft Word or OpenOffice Word) or an image processing program (such as Microsoft Paint or PhotoShop) or email program (Outlook, Hotmail's website) and paste the saved screen into a new document, image, or email.

- **How to capture audio:**

- **Windows Sound Recorder:**

This is an application which is packaged with Windows XP/Vista and enables the user to record any audio being produced by the computer in real-time.

This can enable the user to record audio of an abusive communication or broadcast which may count as evidence in the case of an offense.

The program can be opened by clicking on the Start button, then opening the Accessories folder and finally the Sound Recorder shortcut.

The program is very simple and intuitive. Simply clicking on the Record button initiates the recording of the audio and re-clicking stops the recording. The audio can then be saved in the desired format.

- **How to capture video:**

In the case of encountering video footage which depicts illegal or age-inappropriate acts, the video can be captured using download-helper websites, using Firefox's video-capture extension, or by using commercial software.

The video can then be saved and used as evidence.

- **Download-helper Websites**

KeepVid and YouTube Downloader are download-helper websites that allow users to input the URL of a page which contains a video they wish to download. The website then begins to convert the video into a downloadable format (such as Mpeg or FLV) which can be saved on the hard-drive.

KeepVid (<http://keepvid.com/>)

Youtube Downloader (<http://www.youddl.com/>)

- **Firefox extension**

Mozilla Firefox is a web browser whose Video Downloader extension allows the user to download videos directly off websites. This application runs both on Windows and Mac OS X operating systems.

Mozilla Firefox 3.1

(<http://www.mozilla.com/en-US/firefox/>)

- **Commercial software**

Commercial software is available for purchase and download online. They can be used to capture streaming videos to the computer, with some having the advantage of convert FLV format files into Mpeg or AVI files.

CamStudio (<http://camstudio.org/>)

Replay AV (<http://www.applian.com/replay-av/>)

Social Networking Websites

Social Networking Websites enable the creation of communities in cyberspace. Groups of people who feel that they share the same interests, activities, or simply wish to communicate with other individuals, can use the services of such websites in order to come into contact.

The most popular today are FaceBook, Hi5, MySpace and Bebo. These websites have become specialized in offering people the opportunity to create a sophisticated on-line profile which houses the information they wish to share with the rest of the website's users. Others, such as Second Life, offer users the capability to interact in an unlimited number of ways in a three-dimensional virtual world through their avatars.

This information is usually about their education, where they studied, if they are in a relationship, what their general interests are, and what sort of people they would like to meet. Most websites also allow the users to share photographs, videos and music-playlists through their profiles, as well as blogs, which are essentially electronic journals.

All the users of these websites, especially minors, should be aware that the terms of use may be quite complicated and in some cases may change without the service provider having to notify the users that changes have taken place. This potentially raises the issue of privacy and the safety of one's personal information. There has been increasing controversy regarding this issue because these Social Networking Websites contain huge volumes of information about millions of people around the globe, while the legislation governing personal information in cyberspace remains quite vague.

For this reason, users are advised to keep in mind that Social Networking Websites are very much public and when communicating with other individuals, the same caution should be exercised as when communicating with strangers in the 'real world'. Also, the amount of personal information being shared is recommended to be kept to a minimum.

FaceBook (www.facebook.com):

Facebook (formerly Thefacebook) provides free social networking services through its website. It was founded by Mark Zuckerberg while studying at Harvard University.

The website is meant to emulate that of the facebooks which are given to incoming students, faculty or scholars at universities in order to become acquainted with others. The website's users can browse groups of other users or individuals organized by city, university, region, or occupation, and connect and interact with them. They may add friends (users who can view your entire profile and receive updates regarding your FaceBook activities) send messages, and share various media.

FaceBook has been the center of controversy due to its database being compromised, accusations of selling the information of users to third-parties, as well as changing its terms of use without notifying its users.

It was reported that in June 2008, FaceBook received 132.1 million unique visitors. It is currently the most popular Social Networking Website (and most visited sites) in the world.

MySpace (www.myspace.com):

MySpace allows the creation of personal profiles, blogs, groups, photos, music, and videos. It also allows the design of customizable websites for filmmakers, comedians, and musicians, in order to increase their public exposure.

MySpace is based in Beverly Hills, California, USA and is owned by Fox Interactive Media, itself property of News Corporation. MySpace used to be the world's most popular Social Networking Website, but it was overtaken in monthly visits by its rival FaceBook.

The site hosted approximately 106 million profiles on September 8, 2006. It was noted that during 2006, MySpace attracted 230,000 new users per day.

Second-Life (www.second-life.com):

Second Life is a Virtual World developed by Linden Lab. It was launched in 2003 and is freely-accessible via the Internet by use of a client program called the Second Life Viewer. The program enables users to interact with each other through their fully-customizable personifications in the Virtual World, called avatars. Residents (as the users are called) can explore the world of Second Life, meet others and socialize, participate an infinite number of individual and group activities, and even participate in the Virtual World's economy, which includes the trade of virtual property and services.

Second Life caters for users aged over eighteen, while its sister site Teen Second Life is restricted to users aged between thirteen and eighteen..

Appendices

1. FAQ
2. Lexicon
3. Chat-room terminology
4. Useful software
5. Relevant publications
6. Useful links and contact information
7. Training checklist

Appendix I

FREQUENTLY ASKED QUESTIONS

How do you react if a caller asks for a specific person?

It is important that an understanding is made regarding how to *not* act in such situations. The counselor should not on any occasion state that “such a thing is impossible because it is against the Helpline's regulations” or anything in that manner. Such a reaction is too regimented and authoritarian, which is against the unconditional support ethos of the Helpline and the main reason why children feel comfortable calling in the first place.

A more adequate answer would be a neutral one which will maneuver the issue away from *who* the caller is talking with on to *how* the current counselor may be assistance. For example, the counselor may say in a neutral understanding tone of voice that “I understand that you may feel more comfortable talking to a certain person at this moment; however we are all trained to help you out in the same manner. Is there something that you would like to talk about with me?”

As explained in the section on communication skills, always use the appropriate language for each caller in order to establish rapport.

How do you react if a caller wants to know more about you?

As above, avoid categorical answers and instead opt to a more diplomatic answer, like “I understand that you may like to know more about me but I am here to help you. Knowing more about me will not have an effect on how I may assist you.”

Again, make sure to use the appropriate language. What is the course of action if repeated test calls are being made?

The counselor must remain calm and answer the phone in the customary manner, without showing any signs of irritation in his or her tone of voice. Test calls are exactly that; the caller is dialing the number in order to determine if the counselor is truly someone who is capable of offering support and help. An counselor who answers the phone in an irritated manner or even insults or scolds a caller has failed in this respect. The counselor should answer the phone as many times as it is required, each time as if it is a new caller, expecting that eventually the test caller will decide to talk about any possible issue.

What is the course of action if repeated test calls are being made?

The counselor must remain calm and answer the phone in the customary

manner, without showing any signs of irritation in his or her tone of voice. Test calls are exactly that; the caller is dialing the number in order to determine if the counselor is truly someone who is capable of offering support and help. A counselor who answers the phone in an irritated manner or even insults or scolds a caller has failed in this respect. The counselor should answer the phone as many times as it is required, each time as if it is a new caller, expecting that eventually the test caller will decide to talk about any possible issue.

What to do if you decide that a caller requires on-going psychological support:

The counselor should offer the caller advice regarding the various services which may offer specialized counseling. It is not the Helpline operator's responsibility to arrange appointments or become further involved with this process. The operator's goal is to provide the necessary support in order for the individual to understand the situation and feel confident enough to take action. Although the counselor is expected to offer psychological support, due to the constraint of time, resources and the nature of telephone interaction, it is impossible to offer truly long-term support and for this reason it is rational that the caller be reassured that there are individuals who may help alleviate any long-term anxieties and should be directed to them.

What should be the course of action if you determine that a crime has occurred?

The counselor should offer the caller psychological support in order to reassure that the caller understands and feels that someone can help. Then guidance should be offered on how to report the crime and all the necessary procedures. The counselor should also offer contact information for all the relevant legal institutions whose duty it is to handle such cases.

Are there any cases where it is necessary to breach confidentiality?

Confidentiality is our core value, however this can be breached in two occasions. The first is when a caller states that he or she will or has harmed herself during a phone-call. In such a case, the counselor should try and negotiate in order to talk and possibly delay any self-harm. The counselor must then explain that he or she is legally bound to ask the caller for personal information (name, address, etc.) and then notify the authorities that a person is considering committing suicide or self-harming.

If a Helpline operator reads on a profile that a particular person is considering committing suicide, he or she should notify the website administrator in order to share the information. The Helpline and the administrator can then cooperate in order to notify the authorities and take the necessary precautionary steps.

The only other case where it is necessary to breach confidentiality is when a caller states that he or she plans to harm someone else, or has harmed someone else. The same procedures should be followed.

Where can I find out more about the legislation surrounding Internet use and crimes so that I can have an idea of what constitutes an Internet-crime?

The following URL is a link to a section of the the Cyberethics website (www.Cyberethics.com) which contains all the relevant legislative issues.

(<http://www.cyberethics.info/cyethics2/page.php?pageID=19>)

Appendix II

Lexicon

Anonymous FTP

A means for receiving files from a remote computer without having to have an account with the remote system. Many commercial enterprises maintain anonymous ftp sites for the convenience of their customers so that customers can download updated program files directly to their machines without having to request and receive diskettes through the mail.

Archie

A computer system that manages a database of files that are available on over 1500 computer systems. About 40 Archie servers worldwide share and update the database on a monthly basis.

Blog

There is nothing fundamentally different in the technology that enables blogging as a blog is very similar to other forms of on-line publishing or web sites. However, the blogger makes his or her choice of template as a pre-existing product instead of having to design the look and feel of the page from basics. In the same way that Desk Top Publishing software revolutionised print publication, where content can be dropped into ready made templates, bloggers can put their content into pages that are designed, published and hosted without the blogger needing to know anything about design, marking-up or other technical matters. One major difference, however, is the possibility of adding comments. This was rather difficult technically to achieve in the early days of the web and became more common with the rise of fora and guest books. However, where a forum was usually moderated, a blog is less likely to be so. This encapsulates the definition of Web 2.0. It isn't so very different from Web 1.0, just much easier for individuals with no expertise to get involved. From the point of view of Internet safety, however, the ease of access and use means that it is a technology that enables the dissemination of information and views that might prove undesirable for the audience and the author.

.com

These are commercial sites, which may include corporate homepages or individual users homepages. Commercial sites provide users with reliable information about business enterprises, product information, online technical support for software and hardware, and, in many cases, online product ordering capabilities. Since commercial sites may also provide Internet access to individuals, be wary of sources that have no obvious connection to a business enterprise.

DNS (domain name system)

a system for assigning addresses to computers and people connected to the Internet. The name can be represented both with words and with numbers. Domain name servers "resolve" Internet names and assign numeric addresses so that one computer can find another over the Internet.

.edu

Addresses ending in this extension indicate that you are connecting to a university, college, or other school computer system. These sites can contain both authoritative

and frivolous information, depending on the institution's user policies. If a university grants students, faculty, and staff open access to its Internet system, you can expect to find documents containing anything from research to jokes and humor. Examine documents obtained from educational institutions carefully. Look for department affiliations, author credentials, and any other identifying criteria that would support a document's seriousness and reliability.

Email (electronic mail)

A system for sending and receiving messages on a single computer system or on an interconnection of computer systems, such as the Internet.

FTP (file transfer protocol)

An application that allows users to send and receive files between remote computers. FTP allows a user to save a file to disk, disconnect from the remote system, and then to view or execute the file on the local machine without continuing to maintain a telephone line connection to the remote machine.

GIF (graphical interchange format)

One of several formats used to present images (pictures) over the Internet.

Gopher

A text-based Internet search engine developed by the University of Minnesota. More than 5,000 gopher servers worldwide provide users with subject access to files available over the Internet.

.gov

This extension identifies the information server as a government entity. These sources can be deemed reliable since government bodies (at least in the United States) are charged with the duty of providing their constituents with accurate information on laws, regulations, finances, almost any aspect of government.

Home Page

The opening information provided by a web site. Typically, a home page provides background on the information provider and links to other information sources, both local to the remote computer system and also on other systems worldwide.

HTML (Hypertext Mark-up Language)

A standard for presenting information on the World Wide Web. Documents formatted for html include codes that allow text to be displayed with various fonts, sizes, and attributes as well as instructions to load pictures, sounds, and motion pictures.

HTTP (hypertext transfer protocol)

A set of rules by which information is transmitted across the Internet. HTTP provides a transport system for your local computer to receive data from another computer.

Hyperlink

A link to additional information either within a web document or in other web documents. Hyperlinks are indicated by highlighting and/or underlining within a

web page.

Internet

A world wide interconnection of computer systems that are able to communicate with each other using a common set of protocols. The standard for Internet communication is called TCP/IP. TCP/IP allows computers, regardless of operating systems (DOS, Windows, UNIX, etc.), to exchange data. The Internet had its foundations with ARPANET, an interconnection of computers worldwide that assisted the U.S. Department of Defense to maintain secure contacts worldwide in the event of national emergency.

JPEG (joint photographic experts group)

Another standard for presenting images over the Internet.

.mil

This designates a military body, such as the [Pentagon](#).

MIME (Multipurpose Internet Mail Extensions)

Files available over the Internet may be saved in many formats, including plain text, html, and gif. Web browsers use MIME type definitions to identify file formats.

MPEG (motion picture experts group)

one of several standards for presenting motion pictures over the Internet.

Photo Editing

Editing and enhancing software is now available online and allows users to improve their photos. Examples of this increasingly popular application are:

Picasa (Google)	http://picasa.google.com
iPhoto (Apple)	http://www.apple.com/iphoto
Photo Story (Microsoft)	http://www.microsoft.com/photostory

Photo Sharing

is a popular tool which allows users to share photographs with family and friends. The most widely used site is called Flickr (<http://www.flickr.com>) which allows users to post photos and then invite others to view them either individually or as a slide show. Notes and tags can be added to each photo and others can leave comments too.

Podcast

Podcasting is a way to share multimedia files over the Internet for playback on mobile devices or computers. The term podcast can mean either the broadcast itself or the method of delivery. Anyone with access to the Internet, a microphone and simple computer can create an audio podcast and make it available online. It is possible to subscribe to podcasts so that they will update automatically on a computer or mobile device. In that way, the subscriber will constantly receive new broadcasts as they are updated and produced. It is possible to find server space to store the file (usually mp3) e.g. ourmedia (<http://www.ourmedia.org/>) and to create a podcast-enabled rss feed e.g. feedburner (<http://www.feedburner.com/fb/a/home>)

for free on the Internet.

.org

These are associations or other non-commercial organizations that maintain Internet sites. Much research can be obtained from professional and research organizations. These sites typically will be reliable.

Search Engine

Software that facilitates searching keyword indexes of Internet documents. Well-known Internet search engines include AltaVista, Lycos, HotBot, and Google. Search engines vary widely in their coverage of the Internet, the largest indexing nearly 3.1 billion Web pages. So-called metacrawlers can be used to return top listings from numerous search engines at one time. A more structured means of finding information on the Internet is to use a Web directory like Yahoo or Google Directoy. Directories of Internet content take an approach similar to traditional catalogs and indexes in that they are based on predefined subjects and provide access to materials that, in many cases, have been reviewed.

Social Bookmarking

allows users to share their user-generated Internet favourites or bookmarks. Traditionally users would have a list of favourite websites as part of their own Internet browser. Now, social bookmarking allows these lists to be shared easily so that anyone can use them. The content can be classified using tags to make them easier to search and use. <http://del.icio.us> (owned by Yahoo) is a good example of social bookmarking and shows users how many other people have saved a particular site.

Social Networks

Communities of people who share interests and activities, or who are interested in exploring the interests and activities of others on the Internet. Most social networking websites provide multiple ways for users to interact using chat, messaging, email, video, voice chat, file sharing, blogging, discussion groups and so on. Such sites typify web 2.0, as much of the content is user-generated. They have become very popular very quickly. Bebo attracted 25 million members in little more than a year of operation and generated over 3 billion monthly page views worldwide.

Social networking (SN) sites develop from an initial set of members who send out messages inviting their friends to join the site. New members repeat the process, rapidly increasing the total number of members and links in the network. SN sites offer features such as viewable profiles where users create personal web pages containing personal blogs, photos and other applications that help them to connect with other network members. They also allow users to embed media such as music files and video clips into their profiles and to share their original content with others by uploading it to the site.

These networks tend to be organized around shared common interests. MySpace, for example, builds on independent music scenes. Facebook was originally used exclusively by US Ivy League college students while Bebo and Hi5 make it easy for school and college students to stay in touch with their friends. The value of the

network for its members is linked to the number of people in the network.

There are a number of specifically mobile SNs springing up, such as Dodgeball and Enpresence, which arguably pose more risks for youngsters than Internet based SNs as they notify users when they are in physical proximity to their contacts. Meanwhile the existing web-based SNs are adding mobile services to their offering. Facebook, for instance, offers mobile browsing, photo uploads and the facility to exchange personal messages with other users via SMS (currently US-only) and MySpace is deploying similar services.

TCP/IP (transmission control protocol/Internet protocol)

This set of protocols manages connections between computer systems. Data is sent over TCP/IP in packets, small chunks of data that are keyed to other packets that are needed to complete the transmission of a file. Every document that you view or every file that you receive over the Internet is sent piecemeal via phone using the TCP/IP protocols.

Telnet

An application that allows a user to connect to a remote computer and use it as though the user's computer was a terminal connected directly to it. This includes allowing the user to run programs based on the remote machine. For example, you can connect to LUIS using telnet.

TIFF (tagged image file format)

Another picture format used on the Internet.

TN3270

Telnet 3270 is a form of telnet that makes your computer look like a terminal connected to an IBM mainframe computer. You can reach LUIS, for example, through an Internet connection using TN3270.

URL (uniform resource locator)

The URL identifies to a Web browser the address and type of Internet resource to which your computer is connecting. Types of resources include HTML servers, gopher servers, veronica servers, and ftp servers, each of which has its own set of protocols.

Veronica

A comprehensive, keyword searchable menu of approximately 10,000 Internet sources worldwide. VRML (Virtual Reality Modeling Language)--Still under development, VRML is currently used for three dimensional image representation on the WEB.

Video Sharing

Is a similar tool for sharing videos, with some sites specialized in specific types of video. One of the most popular is youtube <http://www.youtube.com>. A site dedicated to teachers for educational use is teachertube (<http://www.teachertube.com>). Video sharing sites are usually searchable, and allow users to post, comment on, tag and watch videos. A number of communities exist for producing and sharing videos around a common interest. More recently, sites

have appeared which allow users to edit their video clips online and add sound, subtitles and so on. Examples of these include: Jumpcut (<http://www.jumpcut.com>) and VideoEgg (<http://www.videoegg.com>).

Web 2.0

Web 2.0, a phrase coined by O'Reilly Media in 2004, refers to a perceived second-generation of Web-based services—such as social networking sites, wikis, communication tools, and folksonomies - that emphasise online collaboration and sharing among users.

Web 2.0 websites allow users to do more than just retrieve information. They can build on the interactive facilities of "Web 1.0" to provide "Network as platform" computing, which allows users to run software-applications entirely through a browser. Users can own the data on a Web 2.0 site and exercise control over that data. These sites may have an "Architecture of participation" that encourages users to add value to the application as they use it. This offers huge advantages on traditional websites, which limit visitors to viewing and whose content only the site's owner can modify. Web 2.0 sites often feature a rich, user-friendly interface based on Ajax, Flex or similar rich media. The sites may also have social-networking aspects.

Web 2.0 recognises the change from a static to a truly interactive platform. Instead of simply downloading and consuming, users are now able to upload and create. Media is truly converged and no longer separate.

There are several distinctions between Web 1.0 and Web 2.0 as illustrated in the table below.

Web 1.0	Web 2.0
Application based	Web based
Isolated	Collaborative
Offline	Online
Licensed or purchased	Free
Single creator	Multiple collaborators
Proprietary code	Open source
Copyrighted content	Shared content

Four of the most commonly used Web 2.0 technologies are blogs, photo editing, photo sharing, podcasts, social bookmarking, social networks, video sharing and wikis, though a number of other technologies exist.

Remember:

- Web 2.0 tools enable anyone to upload or edit material on the Internet and this may not always be correct or factually accurate.
- Web 2.0 tools offer boundless opportunity for users to publish information about themselves and others. They must nevertheless remain vigilant to the risks of self-disclosure and loss of privacy. The rule of thumb is not to publish anything you don't want the whole world to know about!

- Unlike the traditional web where authorship and ownership of sites was relatively easy to find, the open nature of web 2.0 means that it is more difficult for individual users to know who is behind the avatar. By the same token, as tools for creating and hosting information are widely and freely available, opportunities for posting malicious or misleading information are equally boundless.
- Unlike the real world where some details about who you're talking to cannot be disguised – age and sex for example – this is not true of many of the aspects of web 2.0.
- Information, once posted, cannot completely be removed – web pages are saved by individuals, cached by search engines... Anything you post must be something you could never be ashamed of whether as the author or the subject.
- You or your children are less likely to be stalked or bothered by predators if your computer and web-cam are in a public part of the house and not in the bedroom.
- Remember that although individual pieces of information may not seem to disclose much but when taken together and cross-referenced with friends' information, the whole is greater than the sum of its parts.
- Assume that anything you post will find its way to someone you don't like, and imagine what they can do with that information.

Web Browser

A computer program, like Netscape, Microsoft Internet Explorer, and Mozilla, that can connect to a web server and retrieve information on demand.

Web Crawler

A computerized "robot" that connects to responding computer systems, follows links to documents, and compiles an index of those links and the information available via the links. Also known as "knowbots," some of the most familiar crawlers include WebCrawler and Lycos.

Web Server

A computer system that offers information over the World Wide Web.

Wiki

Wikis are web pages that allow readers to interact and collaborate with others as such pages can be edited or added to by anyone. Perhaps the most well-known example of a wiki is Wikipedia, a collaborative encyclopaedia which now includes more up to date entries than the Encyclopaedia Britannica.

World Wide Web

An interconnection of computer information systems available via the Internet. The Web supports the graphical user interface (GUI) that is so familiar to Macintosh and Windows users. Additionally, the Web can also support sound, pictures, and motion pictures.

Sources: [Greek Safer Internet Awareness Node](#). Copyright © 2007 Extreme Media Solutions Ltd / Safer Internet Hellas & Insafe. Copyright © 2005 European Schoolnet.

Appendix III

Chat room terminology

:) or :-): Smile
;) or ;-): Wink
ASL: Age Sex Location
BF/GF: Boyfriend/Girlfriend
BBL: Be back later
BBS: Be back soon
BRB: Be right back
CD9: Parents are around
GNOC: Get naked on cam
IDK: I don't know
MIRL: Meet in real life
LOL: Laugh out loud
MorF: Male or Female
MOS: Mom over shoulder
NIFOC: Naked in front of computer
Noob: Newbie
NMU: Not much, you?
P911: Parent emergency
PAW: Parents are watching
PIR: Parent in room
POS: Parent over shoulder
PRON: Porn
PRW: Parents are watching
S2R: Send to receive
TDTM: Talk dirty to me
Warez: Pirated Software
W/E: Whatever
WTF: What the f**k?

Check NetLingo, an on-line dictionary of Internet slang and terminology for more.

(<http://www.netlingo.com/>)

Appendix IV

Useful software

Cleaner – A freeware application which cleans your hard-drive and registry of any files which are not part of your system but may have been placed there by malicious software.

(<http://www.ccleaner.com/>)

Spybot Seek & Destroy – A free application which detects any malicious software or spyware which may be lurking on your harddrive or in your memory.

(<http://www.safer-networking.org/index2.html>)

Avast! Antivirus – A freeware antivirus package.

(<http://www.avast.com/>)

Comodo – A freeware firewall application.

(<http://www.personalfirewall.comodo.com/>)

We-Blocker Safe Families software – A free Internet filtering and parental control application.

(<http://www.safefamilies.org/download.php>)

Appendix V

Relevant publications

- Aslanidou, S., & Menexes, G. (2008). Youth and the Internet: Uses and practices in the home. *Computers & Education, 51*, 1375-1391.
- Baumeister, R. F., Heatherton, T. F., & Tice, D. M. (1994). Losing control: How and why people fail at self-regulation. *London, UK: Academic Press.*
- Beebe, T. J., Asche, S. E., Harrison, P. A., & Quinlan, K. B. (2004). Heightened vulnerability and increased risk-taking among adolescent chat room users-results from a statewide school survey. *Journal of Adolescent Health, 35*, 116-123.
- Chou, C., & Peng, H. (2007). Net-friends: Adolescents' attitudes and experiences vs. teachers' concerns. *Computers in Human Behavior, 5*, 2394-2413.
- Chou, C., & Tsai, M. (2007). Gender differences in Taiwan high school students' computer game playing. *Computers in Human Behavior, 23*, 812-824.
- Fisher, D. (1981). Communication in organizations. *New York, NY: South-Western Educational Publishing.*
- Finkelhor, D., Mitchell, K., & Wolak, J. (2001). Highlights of the Youth Internet Safety Survey. Office of Juvenile Justice and Delinquency Prevention.
- Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers. *Systems and humans, 30*, 395-411.
- Gross, E. F. (2004). Adolescent Internet use: What we expect, what teens report. *Journal of Applied Developmental Psychology, 25*, 633-649.
- Hope, J. (2001). Internet Safety: Issues for New Zealand primary schools.
- Li, S., & Chung, T. (2006). Internet function and Internet addictive behavior. *Computers in Human Behavior, 22*, 1067-1071.
- Mesch, G. S. (2009). Social context and communication channels choice among adolescents. *Computers In Human Behavior, 25*, 244-251.
- Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Youth Internet users at risk for the most serious online sexual solicitations. *American Journal of Preventative Medicine, 32*, 532-537.
- Mitchell, K. J., Finkelhor, D., & Wolak, J. (2001). Risk factors for and impact of online sexual solicitation of youth. *Journal of the American Medical Association, 285*, 3010-3015.

- Mittal, V. A., Tessner, K. D., & Walker, E. F. (2007). Elevated social Internet use and schizotypal personality disorder in adolescents. *Schizophrenia Research, 94*, 50-57.
- Tynes, B. M. (2007). Internet Safety Gone Wild: Sacrificing the educational and psychosocial benefits of online social environments. *Journal of adolescent research, 22*, 575-584.
- Valcke, M., Schellens, T., Van Keer, H., & Gerarts, M. (2006). Primary school children's safe and unsafe use of the Internet at home and at school: An exploratory study. *Computers in Human Behavior, 23*, 2838-2850.
- Valentine, G., & Holloway, S. L. (2001). A window on the wider world: Rural children's use of information and communication technologies. *Journal of Rural Studies, 17*, 383-394.
- Wack, E. R., & Tantleff-Dunn, S. (2008). Cyber sexy: Electronic game play and perceptions of attractiveness among college-aged men. *Body Image, 5*, 365-374.
- Whitty, M. T. (2008). Liberating or debilitating: An examination of romantic relationships, sexual relationships and friendships on the Net. *Computers in Human Behavior, 24*, 1837-1850.
- Wolak, J., Mitchell, K. J., & Finkelhor, D. (2003). Escaping or connecting: Characteristics of youth who form close online relationships. *Journal of Adolescence, 26*, 105-119.
- Wolak, J., Finkelhor, D., & Mitchell, K. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health, 35*, 424.
- Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Unwanted and wanted exposure to online pornography in a national sample of youth Internet users. *Pediatrics, 119*, 247-261.
- Ybarra, M. L., Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Internet prevention messages: Targetting the right online behaviors. *Archive of Pediatrics & Adolescent Medicine, 161*, 138-145.
- Yan, Z. (2005). Age differences in children's understanding of the complexity of the Internet. *Journal of Applied Developmental Psychology, 26*, 385-396.
- Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor-targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of child psychology and psychiatry, 45*, 1308-1316.
- Ybarra, M. L., Alexander, C., & Mitchell, K. J. (2005). Depressive symptomatology, youth Internet use, and online interactions: A national survey. *Journal of Adolescent Health, 36*, 9-18.

Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006). Examining Characteristics and Associated Distress related to Internet harassment: Findings from the second Youth Internet Safety Survey. *Pediatrics*, *118*, 1169-1177.

Appendix VI Useful links and contact information

Cyprus

1. ISPs

1. **Spidernet**
(<http://www.spidernet.com/main/default.aspx>)
2. Thunderworx
(<http://www.thunderworx.com/main/default.aspx>)
3. Avacom
(<http://www.avacom.net/>)
4. NewWay
(<http://www.netway.com.cy/>)
5. LogosNet
(<http://www.logosnet.com.cy/>)
6. Cytanet
(<http://www.cytanet.com.cy/>)

2. Local Authorities and Associations

1. Websites of schools (the Internet and educational system in Cyprus)
(<http://www.education.cytanet.com.cy/school.html>)
2. Social welfare services of the Ministry of Labour and Social Insurance
(http://www.mlsi.gov.cy/mlsi/sws/sws.nsf/dmlindex_en/dmlindex_en?OpenDocument)
3. Pancyprian Welfare Council
(<http://www.pwc.com.cy/>)
4. Pancyprian Coordinating Committee of Youth Centers (PCCYC)
(<http://www.pccyc.org/>)
5. Official website of the Republic of Cyprus
(<http://www.cyprus.gov.cy/>)
6. Office of the Commissioner for Personal Data Protection
(http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument)
7. Office of the Commissioner of Electronic Communications & Postal Regulation
(http://www.octpr.org.cy/en_index.htm)
8. Office of the Commissioner for Administration (Ombudsman)
(http://www.ombudsman.gov.cy/Ombudsman/ombudsman.nsf/index_en/index_en?OpenDocument)
9. Ministry of Justice and Public Order
(<http://www.mjpo.gov.cy/>)
10. Ministry of Education and Culture
(<http://www.moec.gov.cy/>)
11. Ministry of the Interior
(<http://moi.gov.cy/>)
12. Ministry of Communications and Works
(<http://www.mcw.gov.cy/>)
13. House of the Representatives
(http://www.parliament.cy/www_START/index.asp)

14. Cyprus Youth Board
(<http://www.youthboard.org.cy/english/default.asp>)
15. Cyprus Police
(<http://www.police.gov.cy/>)
CyberCrime Unit:
Phone # 22-808200, 22-808456, 22-607250
FAX # 22-808465
cybercrime@police.gov.cy
16. Cyprus Consumers Association
(<http://www.cyprusconsumers.org.cy/>)
17. Cyprus Computer Society
(<http://www.ccs.org.cy/>)
18. Competition and Consumer Protection Service (Ministry of
Commerce, Industry and Tourism)
([http://www.mcit.gov.cy/mcit/mcit.nsf/dmlprotect_gr/dmlprotect_gr?
OpenDocument](http://www.mcit.gov.cy/mcit/mcit.nsf/dmlprotect_gr/dmlprotect_gr?OpenDocument))
19. Association of IT teachers of secondary education
([http://www.sykap.com.cy/cgi-bin/banner.cgi?
url=http://www.sykap.com.cy/](http://www.sykap.com.cy/cgi-bin/banner.cgi?url=http://www.sykap.com.cy/))
20. Youth Board of Cyprus
(<http://www.youthboard.org.cy/>)

Europe

Helplines

1. European Association of Internet Helplines, INHOPE
(<http://www.inhope.org/>)
2. Cyberethics, Cyprus
(<http://www.cyberethics.info>)
3. Stoplevel, Austria
(<http://www.stoplevel.at/>)
4. Child Focus, Belgium
(<http://www.childfocus-net-alert.be/>)
5. Red Barnet, Denmark
(<http://www.redbarnet.dk/>)
6. Nettivihje, Finland
(<http://www.nettivilhje.net/>)
7. Point de Contact, France
(<http://www.pointdecontact.net/>)
8. Association of the German Internet Economy Electronic Commerce
Forum, Germany
(<http://www.eco.de/>)
9. FSM, Germany
(<http://www.fsm.de/>)
10. Jugendschutz, Germany
(<http://www.jugendschutz.net/>)
11. SafeLine, Greece
(<http://www.safeline.gr/>)

12. Internet child pornography hotline, Ireland
(<http://www.hotline.ie/>)
13. Stop-It, Italy
(<http://www.stop-it.org/>)
14. Meldpunt, Netherlands
(<http://www.meldpunt.org/>)
15. NIFC Hotline, Poland
(<http://www.hotline.org.pl/>)
16. Protegeles, Spain
(<http://www.protegeles.com/>)
17. Radda Berner, Sweden
(<http://www.rb.se/>)
18. Internet Watch Foundation, United Kingdom
(<http://www.iwf.org.uk/>)
19. ChildLine, UK
(<http://www.childline.org.uk/Pages/default.aspx>)
20. Helpline.org.pl, Poland
(www.helpline.org.pl)

Awareness Nodes

21. Austria
(<http://www.saferInternet.at/>)
22. Belgium
(<http://www.saferInternet.be/>)
23. Czech Republic
(<http://www.safer-Internet.cz/home.asp?idk=1>)
24. Denmark
(<http://andk.medieraadet.dk/>)
25. Finland
(<http://www.tiukula.fi/>)
26. France
(<http://www.Internetsanscrainte.fr/>)
27. Germany
(<http://www.klicksafe.de/>)
28. Greece
(<http://www.saferInternet.gr/>)
29. Hungary
(<http://www.baratsagosInternet.hu/mss/alpha>)
30. Iceland
(<http://www.heimiliogskoli.is/>)
31. Ireland
(<http://www.ncte.ie/InternetSafety/>)
32. Italy
(<http://www.easy4.it/>)
33. New Zealand
(<http://www.netsafe.org.nz/>)
34. Lithuania
(<http://www.draugiskasInternetas.lt/lt>)
35. Holland
(<http://www.digibewust.nl/>)
36. Norway

- [\(http://www.saftonline.no/\)](http://www.saftonline.no/)
37. Poland
(<http://www.saferInternet.pl/>)
 38. Portugal
(<http://www.Internetsegura.pt/>)
 39. Slovenia
(<http://english.safe.si/>)
 40. Spain
(<http://www.protegeles.com/>)
 41. Sweden
(<http://www.medieradet.se/>)
 42. United Kingdom
(<http://www.uclan.ac.uk/>)
 43. European Network of E-Safety Awareness Nodes, INSAFE
(<http://www.saferInternet.org/>)
 44. EU page on cyber-bullying
<http://www.keepcontrol.eu/>
 45. SafeBorders
(<http://www.safer-Internet.net/>)
 46. European Research Into Consumer Affairs
(<http://www.net-consumers.org/>)
 47. Safety, Awareness, Facts and Tools
(<http://www.saftonline.org/>)
 48. Safer Internet for Knowing and Living
(<http://www.sifkal.org/>)
 49. Safer Use of Services on the Internet
(<http://www.besafeonline.org/>)
 50. EuroPol
(<http://www.europol.europa.eu/>)
 51. EICN – European Internet Coregulation Network
(<http://www.Internet-coregulation.org/>)
 52. European Commission's page on Internet safety.
(http://ec.europa.eu/information_society/activities/sip/index_en.htm)
 53. QuickLinks – Links to news items about legal and regulatory aspects of the Internet and the information society
(<http://www.qlinks.net/>)
 54. SIP – Official Documentation on the “Safer Internet Programme”
(http://ec.europa.eu/information_society/activities/sip/index_en.htm)

International

Helplines and awareness nodes

55. NetAlert, Australia
(<http://www.netalert.net.au/>)
56. Australian Broadcasting Authority, Australia
(<http://www.aba.gov.au/>)
57. Barnaheill, Iceland
(<http://www.barnaheill.is/>)
58. Ecpat Taiwan, Taiwan
(<http://www.web547.org.tw/>)

59. National Center for Missing and Exploited Children, USA
(<http://www.ncmec.org/>)
60. i-Safe, USA
(<http://www.i-safe.org/>)
61. NetSmartz, USA
(<http://www.netsmartz.org/>)
62. United Nations Childrens Fund, UNICEF
(<http://www.unicef.org/>)
63. Interpol
(<http://www.interpol.int/>)
64. Office of the United Nations High Commissioner on Human Rights
(<http://www.ohchr.org/>)

Appendix VII Training checklist

We have compiled below a checklist for potential volunteers to ensure that they have studied all materials and have acquainted themselves with all relevant information.

1	Have you studied in detail our website?	
2	Have you studied this Training Manual?	
3	Did you watch all the training videos which we have available in the Training Section of the Helpline website?	
4	Do you know who is who at CyberEthics and have you met all key people?	
5	Are you familiar with computer and Internet terminology?	
6	Do you know how to find the administrator of a domain?	
7	Do you have experience with communication via MSN, Skype, AIM, etc. and is your knowledge enough to provide guidance on a specific function?	
8	Do you have sufficient experience with social networking sites such as MySpace, FaceBook, Hi5, etc.?	
9	Do you know how to utilize the Print-Screen functions or how to capture videos from the Internet?	
10	Do you know who the Internet service providers are in Cyprus and how to contact them?	
11	Do you know all the relevant websites referenced in this Manual and how to navigate through them?	
12	Do you know where to find further information?	