



# CONTENTS

<b>Introduction</b>	<b>3</b>
<b>Study Methodology</b>	<b>3</b>
<b>Definitions</b>	<b>5</b>
<b>Key Findings at a Glance</b>	<b>5</b>
• Cyber Addiction	5
• Cyber Bullying	5
• Cyber Exploitation	5
<b>Additional Findings from International Studies</b>	<b>5</b>
• Cyber Addiction	5
• Cyber Bullying	6
• Cyber Exploitation	6
<b>Analysis</b>	<b>7</b>
• Cyber Addiction: How it Started	7
• Cyber Addiction: Why it is a Problem	8
• Cyber Addiction: Recommendations	10
• Cyber Bullying: How it Started	12
• Cyber Bullying: Why it is a Problem	15
• Cyber Bullying: Recommendations	16
- Making Cyber Bullying Illegal	16
- Synchronising and Collaborating with Concerned Government Authorities	17
- Creating Lesson Plans (Teachers)	18
- Creating Homework Assignments for the Betterment of Society (Teachers)	18
- Offering Access to Guidance Counsellors for Children	19
- Addressing the Issues Directly with Your Child and Their Teachers (Parents)	20
- Staying Abreast with Social Media "Terms and Conditions" Policies (Parents)	20
- Providing Access to Hotlines and Other Tools for Anonymous Victims and Good Samaritans (Government)	22
- Calling for Help with the Click of a Button	23
• Cyber Exploitation: How it Started	24
- The Disparity between Parents and Children about Online Activity	25
- "Over-Sharing" Information: How Much is Too Much?	26
- Location-Based Services	26
• Cyber Exploitation: Why it is a Problem	27
• Cyber Exploitation: Recommendations	28
- Creating a National/Regional Online Predator Registry Website	28
- Case: A Robot Exposing Indecent Exposure	28
- Refer to Lists of Recommendations Provided by Online Resources	29
<b>Conclusion</b>	<b>31</b>
<b>Call-to-Action</b>	<b>33</b>
<b>Acknowledgment</b>	<b>34</b>
<b>References</b>	<b>35</b>

## INTRODUCTION

The ever-evolving Information Age is serving our youth for multiple purposes, particularly with regards to education and social media. Contrary to adults, who primarily use it for work-related activities, most young people perceive it to be a fundamental necessity to their daily lives. They use it for entertainment, socialising with others and-- perhaps the most important and least controllable aspect of all-- developing an identity. As a result, this can potentially impact some or all elements of youths' health: physical, mental, social, emotional, intellectual and sometimes even spiritual.

Contrary to how children in the GCC region interacted up to 10 years ago, social media platforms have now become a substitute for face-to-face interactions. They have provided an easy way to show social status visible on-screen and people's actions can now be tracked tangibly. This is just one of the various life aspects minors are naive about when using the Internet, which is why we must continue providing a continuous discourse on social media's implications.

Although there has been significant regional research done on social media, there has been very little discourse on how it relates to cyber safety. As a result, very few people in the Arab World are not aware of how social media and the constant usage of electronic devices have not only created a wider scope of problems for the younger generation, but they have also triggered issues that started offline. Furthermore, because very little has been done institutionally to tackle the issue, the prevalence of these cyber risks is dramatically increasing, leaving adults around the world deeply concerned. In essence, it is important for policymakers, educators and parents to be aware of Internet-related issues that violate a child's cyber safety, along with the risks associated with them.

The purpose of this report is to investigate to what extent children:

- (1) Access the Internet (how, when and where)
- (2) Are aware of how long they spend online and the risks of cyber addiction
- (3) Are aware of cyber bullying, its frequency and what forms of cyber bullying they experience
- (4) Communicate with parents, teachers and government authorities about cyber safety
- (5) Take responsibility for their safety on the Internet

In addition to ICDL's Summer Camp study, this report will provide recommendations in the "Analysis" section for government authorities, teachers, and parents **(starting on pages 7, 12 and 24 for cyber addiction, cyber bullying and cyber exploitation, respectively)**.

## STUDY METHODOLOGY

Every year, ICDL Arabia commissions a cross-sectional study of their Summer Camp participants in the UAE. A survey consisting of 20 multiple-choice questions designed by the ICDL Arabia team is distributed to 404 adolescents (64% female, 36% male) aged range of 14 and 18 in an effort to learn more about their personal experiences while using the Internet. These students lived in 6 of the 7 emirates of the UAE and were predominantly Emirati.

Respondents were assured that their identities would remain confidential and the survey was conducted and supervised by the ICDL Arabia quality assurance team as well as a certified trainer for the purposes of clarifying questions.

The surveys were administered on the 13th of July, 2014 until 28 August 2014 to all Summer Camp participants in the UAE and they were required to finish the survey before they completed a test with ICDL's Social Media Essentials course.

## DEFINITIONS

**Cyber Addiction** - any online-related compulsive urges and behaviours, which interfere with other daily activities.

**Cyber Bullying** - the use of electronic communication to harass, intimidate, or threaten a person.

**Cyber (Child) Exploitation** - child grooming by online predators or Internet stalkers through the use of false online identities or through accessing personal information published on the internet.

**Trolling** - refers to when someone sends a message online with the intention of causing a negative reaction.

**Flaming** takes place when a bully repeatedly sends an offensive message intended to invoke certain emotions, targeted to a specific person or group.

**Masquerading** - a person who pretends to be the actual victim and post negative content in an attempt to make that person look bad or place him/her in danger.

**Hacking** - a common process by which people with suitable 'coding' skills can gain unauthorised access to personal electronic devices, most commonly computers, servers and mobile phones.

**Phishing** - Any email, text message, or fake website created to look like it's from an authentic company

**Pharming** - A practice in which malicious code is installed on an electronic device that misdirects users to a malevolent and illegitimate website.

**Location Based Services - Geo Tagging** - the process of adding geographical identification meta data such as longitude and latitude to media such as photographs, videos, websites, SMS message or QR (quick response) code for the purpose of identifying the location that the media was created at. Used in many social media networks and mobile applications.

**GCC countries** - The GCC member states are: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates.

**Arab World** - The 22 Arab speaking countries of the Arab League

**Arab Government** - Any Government of one of the Arab League countries

**MENA** - geographical region covering the Middle East and North Africa

**Selfie** - A popular adolescent practise of taking photos or video of yourself and posting on social media

**Online predators** - any person, male or female using the internet for the express purpose of targeting a minor for child exploitation

## KEY FINDINGS AT A GLANCE

### 1. Cyber Addiction

- ✧ There is an increasing use of portable devices used by youth when accessing the Internet: 26% of them use a smartphone and 37% of them use a tablet.
- ✧ 81% of respondents said that others complain about the amount of time they spend online (48% sometimes, 33% often).
- ✧ 85% of youth stay in touch with their friends and family using Instant Messaging platforms.

### 2. Cyber Bullying

- ✧ 60% of GCC youth openly admit to the presence of cyber bullying amongst their peers.
- ✧ 26% of adolescents felt it was unlikely that that a parent or teacher could assist them if they are to face an online problem.
- ✧ 54% of UAE adolescents are not aware that cyber bullying is a crime punishable by law.
- ✧ 64% of those interviewed do not know or are unsure of what cyber bullying is.
- ✧ Only 12% believe that they think cyber bullying happens "all the time" and 23% believe that cyber bullying "never happens."

### 3. Cyber Exploitation

- ✧ Nearly half (48%) of adolescents spend the majority of their Internet usage in the privacy of their bedrooms with no adult supervision.
- ✧ 16% of those surveyed have received online requests for private or personal information from a stranger
- ✧ 16% of those surveyed have received inappropriate online content (website links, photos, videos, etc.)

## ● ADDITIONAL FINDINGS FROM INTERNATIONAL STUDIES

In addition, due to the lack of regional research, this report also examined whether the survey results correlated with studies carried out elsewhere in the world.

### 1. Cyber Addiction

- ✧ Over 20% of 8 to 18-year-olds in the United States use the Internet for more than 16 hours every day; this includes the use of any electronic device with access to the Internet.
- ✧ With the mass adoption of portable devices, we are seeing a high correlation between people who own these gadgets and Internet reliance.
- ✧ As more pre-teens are being exposed to the Internet, there is a higher risk of being cyber-addicted at an early age.
- ✧ Countries with an overall substandard life satisfaction, greater overall pollution and greater traffic commute time consumption are considered factors that contribute to cyber addiction.

## 2. Cyber Bullying

- ※ Only 1 in 4 teenagers who bully others online have bullied others offline, suggesting that bullying on the Internet is a much larger threat to youth than face-to-face bullying.
- ※ Most developed countries have very thorough governmental and educational policies in place with language specifically relating to cyber bullying.
- ※ A wide variety of strategies in government, schools and households have been implemented to combat cyber bullying around the world.

## 3. Cyber Exploitation

- ※ 750,000 paedophiles are online at any given moment.
- ※ 41% of parents allow their kids to use a gaming console unsupervised; 40% allow them unsupervised access to a computer; and 29% allow their kids under age seven to use mobile apps unsupervised.
- ※ There is a disparity between generations' perceptions of how parents monitor their kids' online activity: 39% of teens said their parents monitored their activities closely, compared to 84% of parents who were asked the same question.
- ※ 78% of former burglars strongly believe social media platforms are being used by current thieves to burglarise personal properties.

## ANALYSIS

### 📍 CYBER ADDICTION: HOW IT STARTED



**Cyber addiction is the excessive compulsive non-productive use of the Internet by an individual desperately relying on it to occupy free time for recreation or social purposes.**

ICDL Arabia

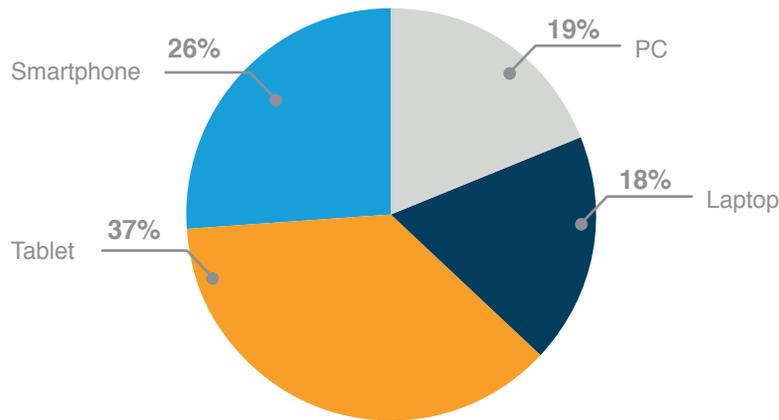
The phenomenon of cyber addiction has become so rampant, yet because it is a relatively new phenomenon its definition is still under discussion. With the increasing availability of Internet access, more youth are becoming more tech-savvy while progressively spending more time interacting on social media and utilising applications on electronic devices, which in turn takes a toll on their offline lives. While time spent online can be beneficial, several studies have indicated that compulsive Internet use can interfere with a child's daily life activities, schoolwork and relationships. The Kaiser Family Foundation, a well-respected thought-leading non-profit organization on health policy analysis in the U.S. that produces a report of 8-18 year olds' media usage every five years, reported youth who spend more than 16+ hours on media outlets every day and do not use the Internet in moderation, reported lower grades and a higher likelihood of boredom, sadness and mischief.<sup>i</sup>

As we enter into the second half of the 2010's decade, the Internet is becoming more accessible to youth than ever before. This is especially true in the GCC region, where Internet penetration rates are among the highest in the world: Bahrain, Qatar and the UAE are in the world's top 10, with Internet penetration rates of 98.7%, 95.0% and 95.7% respectively. Compare this to the number of users in 2005, when the Arab World made up only 1% of global Internet users and only 18 computers were available per 1,000 people compared to the average of 78 per 1,000 today.<sup>ii</sup> In 2002, only 6 percent of all women in the Arab World had access to the Internet.<sup>iii</sup> Today, because the Internet is considered an essential communication platform for people around the world, public and private entities from all industries are investing more time and money in Internet bandwidth and encouraging the use of digital forms of communication.

One of the predominant effects of increased investment in Internet-related activities is the mass adoption of portable devices. Take the iPhone, for example: when it was introduced in 2007, we saw a vast increase in demand for WiFi connectivity, as people increasingly demanded Internet access wherever they go. Similarly, when the iPad came out in 2010, it re-shaped the commercial market calling for more portable technological devices with access to the Internet. In fact, a 2013 Ofcom report indicated that tablet devices are becoming increasingly popular for pre-teens.<sup>iv</sup> Regardless, if a person frequently used a laptop or desktop computer, they have now been given a cheaper and more feasible option to use the Internet.

This correlates well with our study's findings. As seen in **Figure 1**, youth's main preference for using the Internet is quite diverse: 26% would access it most through smartphones, 37% prefer to use a tablet, 19% have a preference for desktops and only 18% would use a laptop.

**On which device do you spend the most time on the Internet?**



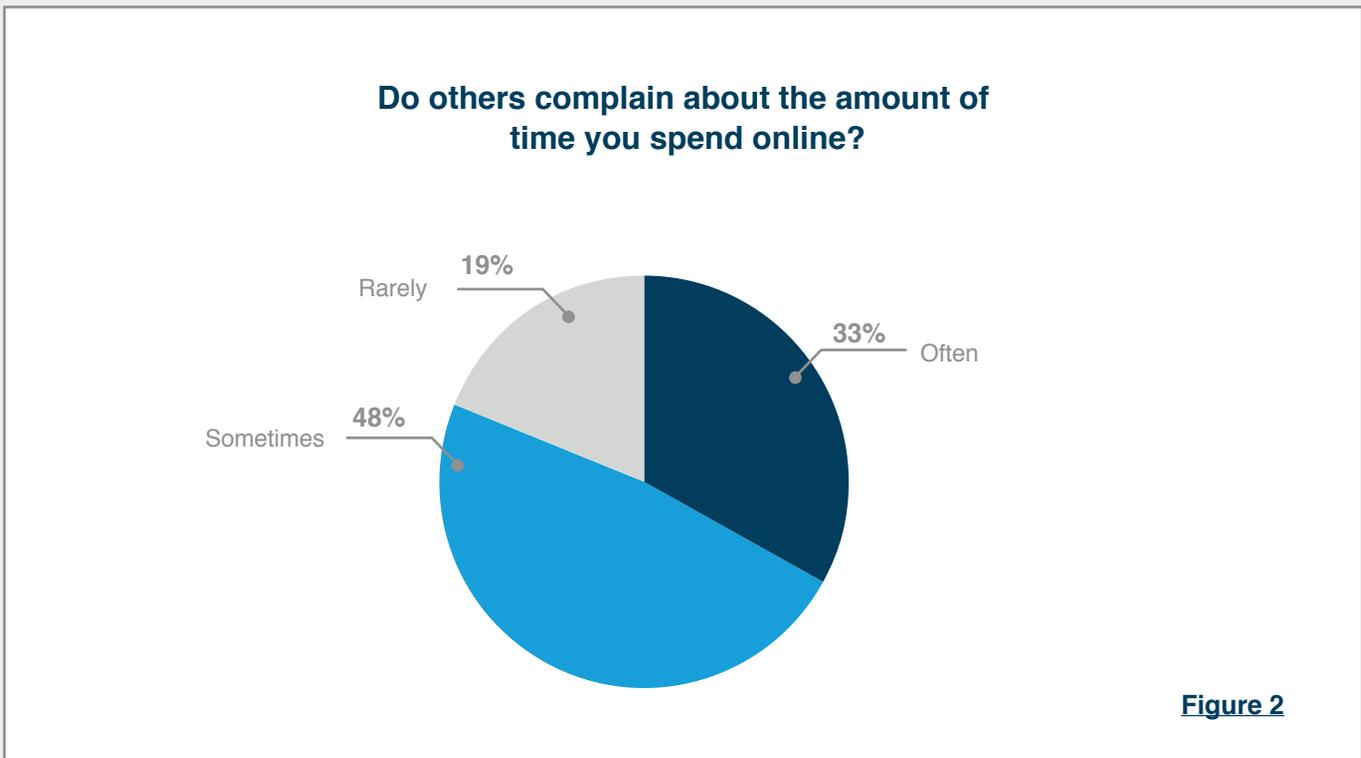
**Figure 1**

**● CYBER ADDICTION: WHY IT IS A PROBLEM**

Due to our heavy reliance on the Internet, the proportion of those who spend more time online than offline is becoming lopsided. Many youth look to the Internet as a way to escape from reality. A freedom from real-life problems, it is considered an outlet to eliminate any stress, depression, anxiety and/or any other unpleasant feelings.<sup>v</sup> It eventually becomes a habit to go online because, in a way, the Internet gives a platform to escape these difficult feelings.<sup>v</sup> This may seem like an appropriate way to fix the problem in the short run, however a continuous reliance on it eventually gives people the false notion that they need the Internet even more, because the negative emotions are only elongated and never resolved.

As of 2014, 6% of the world's population is now affected by cyber addiction<sup>vi</sup> and it is starting to become more prevalent in certain areas. Look no further than the GCC region as an example of just how toxic cyber addiction can be. Taking into account that GCC countries have very high Internet penetration rates, they are also among the highest prevalent regions of Internet addiction (10.9% compared to 2.6% in Western and Northern Europe). According to the U.S. journal *Cyberpsychology, Behavior and Social Networking*; they concluded that countries with less life satisfaction, greater overall pollution and greater traffic commute time consumption, were all factors that contributed to the condition's prevalence.<sup>vii</sup>

81% of ICDL Arabia's Summer Camp participants stated that others complain about the amount of time they spend online (33% often, 48% sometimes; See Figure 2), inferring that several people are aware of how much time youth in the Middle East spend online. Nonetheless, nothing has been done to combat or even declare this as an issue in most GCC countries. On an international level, this has been considered a clinical disorder in China since 2008. Japanese policymakers have created "Internet fasting camps" where young teens explore natural environments while avoiding anything digital in an attempt to help them discover a more traditional lifestyle.



South Korea is considered to be at the forefront of this issue, as they have been battling this issue the longest. Since 2002, eight different ministries developed a Master Plan designed to affect their citizens on a national level. They offered several opportunities that the Middle East can emulate, including the opening of an Internet Addiction Prevention and Counselling Centre in 2002 (the first of its kind). As of today, they have created a second series of projects, many related to newer technological concepts such as smartphone technology and the usage of apps.

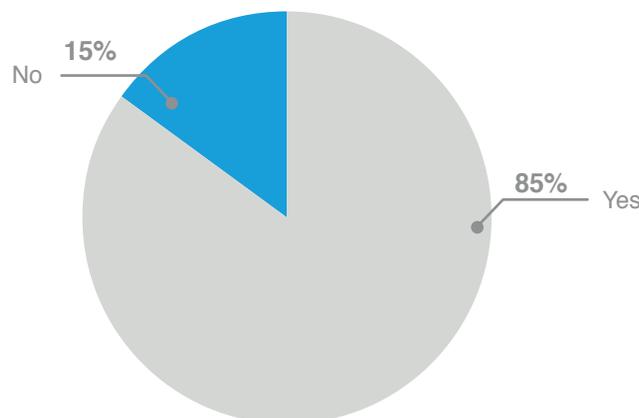
These rehabilitation programmes can easily be replicated in the Middle East and, if implemented well, could be an effective and practical supplement for traditional therapeutic ways to battle cyber addiction. However, it should not be a substitute method for those who have just begun to lose control of their online activity. It would help adolescents gain essential skills for the real world, particularly skills related to face-to-face communication and analysing their online/offline balance.

## 🕒 CYBER ADDICTION: RECOMMENDATIONS

In a "multitasking" world where many of us are guilty of texting or checking our social media accounts while conversing with someone face-to-face, kids can be even more prone to this relatively new wave of distractions. Arguably, the most common reason for excessive Internet usage among youth is boredom. The quickest and easiest solution most youth have used in the 21st century to fill their time has been to log onto one of their social media accounts and to occupy themselves in a world full of information and entertainment.

A more traditional outlet has been the usage of text messaging. Surely, this has been a way of keeping in touch with close friends and family members for decades now, but society has reached a point where texting to someone in the virtual world has supplanted conversations with people in the same room. ICDL's Summer Camp survey (**See Figure 3**) suggests that an overwhelming 85% use instant messaging platforms. More studies need to be conducted in the Arab World to find out how much time children of all ages spend using these applications and whether people consider it a primary or alternative method of communication.

### Do you use Instant Messaging? (Eg: BBM, WhatsApp, etc.)



**Figure 3**

Many have wondered how a concept so simple yet so embedded into our society can be traced. One ironic answer many families and teachers have utilised is to use apps to fight against the overuse of technology. One of such tool used in today's era is the "Self-Control" app, which can be a very useful tool to help combat youths' distractions and assist them in using the Internet productively. School administrators could download the app and use it on school computers, while parents could learn how to utilise it in the household.

Once this type of app is downloaded, teachers and parents have the opportunity to add certain websites to **blacklists**<sup>viii</sup> (what the app uses to classify distracting websites). After creating the list, an appropriate time can be set for how long it should take to complete an assignment, or until they need a much-deserved break. Inversely, there is also the option of a **whitelist**, which gives adults the ability to include web addresses that can be allowed to be used at a given time; the app will then block all other Internet connectivity. This can be done on multiple electronic devices, including laptops, smartphones and tablets.

This type of app, of course, will not work unless there is a responsible adult present at home, who understands how the app works. Getting a parent or a guardian involved in a student's online schoolwork is vital in this day and age. A teacher can provide a contract for a student's parent to sign and brought back to the teacher ensuring that they understand the rules or engage the parents through a cyber-addiction workshop so that parents understand the reasons behind the app and are fully engaged with using it.

## ④ CYBER BULLYING: HOW IT STARTED



**Cyber bullying is the use of threatening or mean language on social media platforms, chat rooms, or any other means of information technology to purposely harass or emotionally hurt a single person or a group of people.**

ICDL Arabia

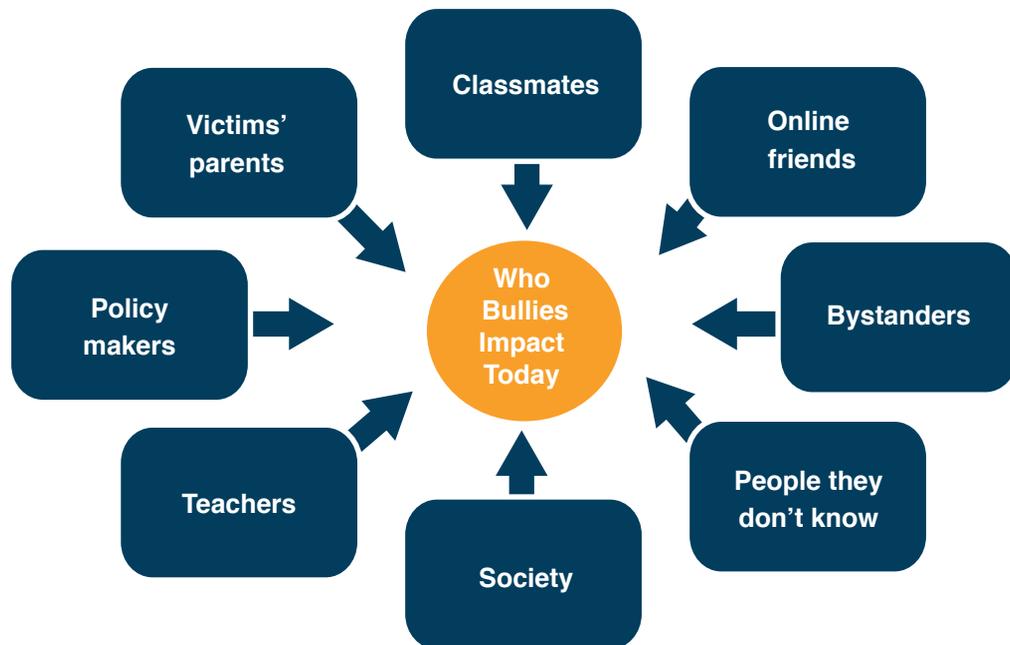
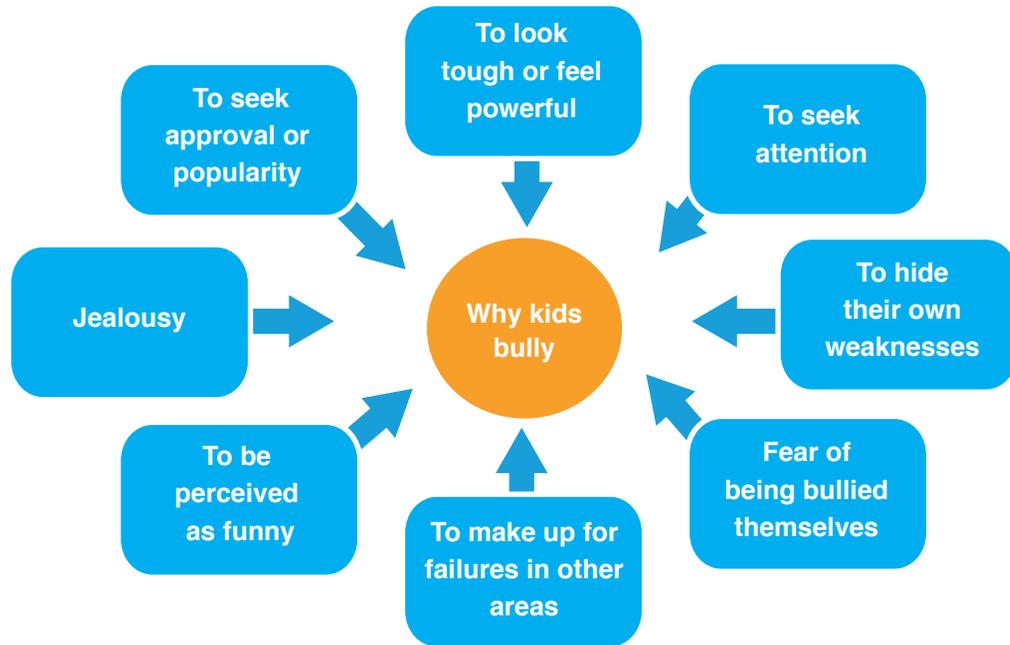
Traditionally, most school-related bullying took place exclusively on the school playground and victims could usually rely upon their homes as sanctuaries to escape it. Although face-to-face bullying still takes place within the school setting, most bullying has converted into an electric form via online platforms. With most students now making it a daily habit to check their social media accounts, they are consequently more prone to facing problematic situations that lead to cyber bullying, a form of bullying that has no safe haven.

Relating to this is our urge to create paradigm-shifting perspectives on cyber bullying. Several studies, particularly ones in the Western World, put an emphasis on the victims, how they are affected by it and what they can do to overcome it. Yes, cyberbullies' targets need support, but this creates a very narrow-minded effect in how the mass population thinks about the issue. What we do not address is how the holistic culture of online communication perpetuates cyber bullying, along with the several reasons for why people bully in the first place. In essence, this affects everyone online.

※ Witnesses of cyber bullying consciously choose not to report cases of cyber bullying that do not directly involve them; bystanders unknowingly represent a social consensus, so they have an important role to play in stopping these vicious acts.

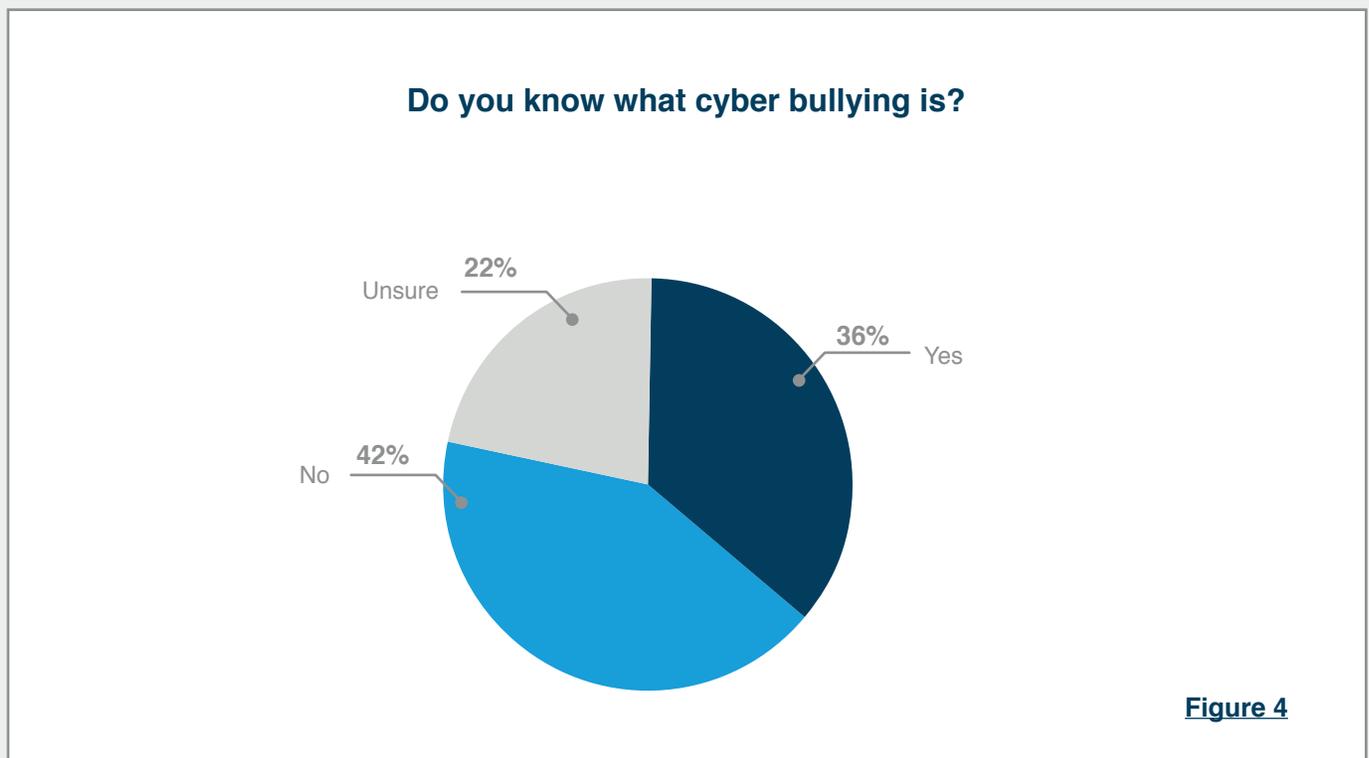
※ A significant percentage of youth who claim to have been victims of cyber bullying end up becoming bullies themselves.<sup>ix</sup>

※ Cyber bullying at an early age affects the bully, as well: not only are they less likely to learn important life skills (such as compromising), but they also have a higher chance of skipping or dropping out of school completely<sup>x</sup>, getting in physical fights and being convicted of a crime by age 24.<sup>xi</sup>



Expanding our conversations about cyber bullying and shifting our focus on the way everyone interacts online ultimately impacts how youths interact offline. It also calls attention to two main ideas. Firstly, it changes our cognitive structure on how we talk about cyber bullying, as it recognises that it is a systematic social problem. Secondly, it acknowledges that this is not just a problem only some of us need to fix. This is an ongoing problem where the language we use is both part of the problem and part of the solution. As thought leaders on cyber bullying, the words we currently use subconsciously conspire to thinking only about what victims need to do to protect themselves. Talking about victims' safety is important, but we also need to address how this impacts everyone online, particularly those minors who are in the midst of finding his/her online identity.

It is quite clear that this particular cyber issue is not being discussed enough as it should. As a result, many adolescents are not aware of how often cyber bullying occurs, nor are they aware of the potential consequences their actions have on both their peers' and their very own lives. 64% of those interviewed in the ICDL Summer Camp survey either do not know or are unsure of what cyber bullying is (**See Figure 4**). This is a frightening statistic and emphasises a desperate need for education on this subject throughout the Arab World.



## ● CYBER BULLYING: WHY IT IS A PROBLEM

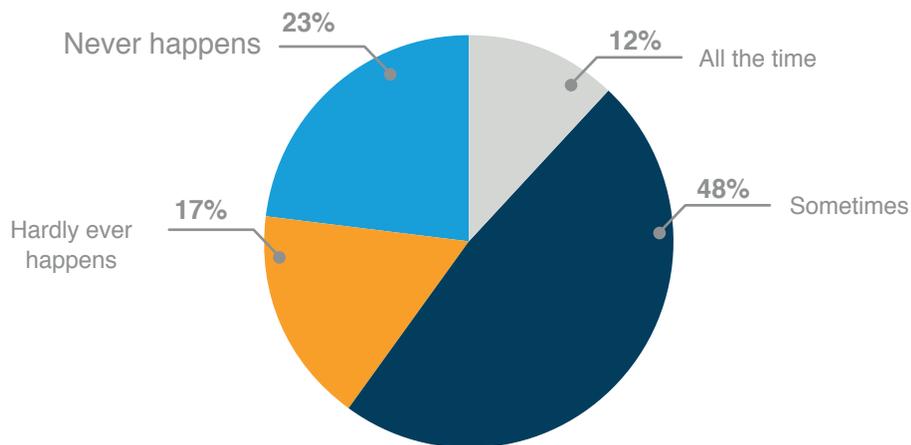
While rates of peer victimization (and its effects) have been widely researched by European and North American countries for decades, cyber bullying in the Arab World is, in contrast, a more recent phenomenon. Studies on the matter within the GCC region are difficult to find, particularly with regards to the impact cyber bullying has on schools. Nevertheless, out of the studies that currently exist on the subject (as of 2014), 20.9% of middle-school adolescents report bullying in the UAE; the same goes for 39.1% in Oman.<sup>xii</sup> Typically, boys concur with this form of harassment more than girls.

Our lack of regional research and education on the negative consequences of cyber bullying implies that we are downplaying the issue. Studies from world-renowned organizations have discussed how online bullying negatively impacts a wide array of life aspects, similar to traditional forms of bullying, including, but not limited to, self-esteem, social life, optimism for the future, academic studies, relationships with family members, career plan aspirations and can ultimately lead to considerations of suicide. Keeping that in mind, cyber bullying has created a wider scope of problems. Nancy Willard of the American non-profit *Responsible Netizen Institute* explained that technology now has the power to affect a young person's ethical behaviour.<sup>xiii</sup>

Because the Internet is still a relatively new medium of communication and due to a lack of guidance and feedback from a responsible adult, young Internet users are unaware in most cases of the consequences of their actions to others online, which in turn minimises their feelings of empathy and remorse for one another. Canadian cyber safety programme *Be Web Aware* suggests that there is evidence that only a quarter of teenagers who cyber bully others have bullied others offline.<sup>xiv</sup> This means that, because people have the power to be anonymous and are able to hide their true identity, the virtual world has empowered the remaining three quarters who would not have considered bullying anyone in the physical world. Furthermore, it signifies that the Internet has formed a tenacious relationship with bullying and it will only worsen with time if nothing is done to combat the issue. In essence, it is the 'cyber' in cyber bullying that makes this issue more prevalent.

With the rise of Internet usage across the globe and very little being done to prevent its negative effects, it is no surprise that cyber bullying is on the rise. Nevertheless, the majority of the ICDL Summer Camp survey's respondents do not think so. Our results indicate that only 12% believe that cyber bullying happens all the time. An even more surprising statistic is that nearly one in four respondents (23%) believe that cyber bullying "never happens." (**See Figure 5**). The inference for this is those who do not believe cyber bullying happens often dismiss what they cannot see. Most people have probably witnessed and may have even been affected by cyber bullying without realising it.

### How often do you think cyber bullying happens?



**Figure 5**

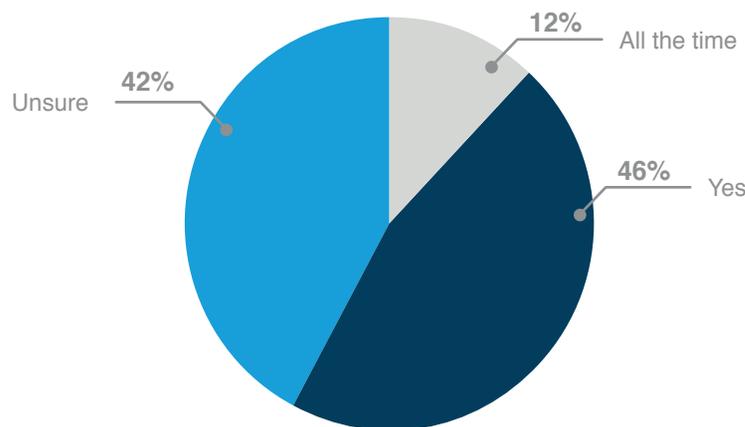
## 🌐 CYBER BULLYING: RECOMMENDATIONS

### 1- Making Cyber Bullying Illegal

With the idea that cyber bullying has a larger impact on a young person’s social life outside school grounds, governments need to develop and enforce policies that prevent and remove its source. Policies are written with the intention not only to unify a general population on issues that affect others, but also to prevent such instances from occurring. Integrating new laws that add consequences on cyber bullying is a step in the right direction for creating a safer online culture for all digital citizens in the region. To give an example, in the UAE, defamation, which includes written posts on social media that are proven libellous, carries up to a 2-year prison sentence.<sup>xv</sup>

The result of the ICDL Summer Camp survey confirms that a large proportion of adolescents in the UAE are not aware that cyber bullying is a crime punishable by law: less than half of the sample answered yes and an astounding 42% said no to this question (See Figure 6).

**Did you know that cyber bullying is a crime punishable by law?**



**Figure 6**

**2- Synchronising and Collaborating with Concerned Government Authorities**

Contrary to public opinion, legal policies are not just meant to be examined by the Interior Ministries. As cyber bullying becomes more widespread, more aspects of cyber bullying are taken into account, which calls for different sectors of government. The Ministry of Education, for example, has the duty to implement policies that encourage teachers to create lesson plans around cyber bullying. Also, given the social implications and health-related consequences of cyber bullying, health departments are becoming definitive resources to help fund mental health research on cyber bullying.

The Australian Government’s Department of Education and Training<sup>xvi</sup> collaborated with the National Health and Medical Research Council along with the Centre for Emotional Health at Macquarie University to support a recent research study examining different anti-bullying campaigns. They have also contributed funds for studies aiming to gather information about what schools are currently doing to proactively and reactively counter bullying. They have established solid partnerships with reputable universities and are allocating more resources every year to reach out to hundreds of secondary schools and thousands of students.

The United States' Department of Health & Human Services has, at a federal level, created the website StopBullying.gov, which provides an educational online resource for prevention and education on how to respond to any form of bullying. It includes sections to allow for the different age groups providing age appropriate guidelines as well as a page targeted for young adults and college students. A tab specifically addresses cyber bullying, which is divided into three parts: **explanations** for how it is different from traditional forms of bullying, tips on how to **prevent** it (directed to children and their parents) and the correct steps to take when a person wants to **report** a case of cyber bullying.

### 3- Creating Lesson Plans (Teachers)

Naturally, talking about bullying online is going to be difficult if schools and teachers do not include it in a structural format. Teachers creating lesson plans would help begin this process, as it strengthens students' acknowledgment that the issue exists and why it is critically important to learn. With an aim to educate kids at an institutional level about a subject that directly impacts them outside the classroom, these open discussions can help build trust between student and teacher over time.

Typically, teachers who understand the impacts of cyber bullying incorporate different activities in their curriculum, including videos, games and real-life scenarios for students to analyse. Refer to Digizen<sup>xvii</sup> and Common Sense Media<sup>xviii</sup> for examples of lesson plans in cyber bullying.

Schools should look to create a team leader with the responsibility of ensuring that all teachers have sufficient training in what to look out for and also to create the content for lesson plans or address the issue in a special assembly, not forgetting parent/teacher conferences.

### 4- Creating Homework Assignments for the Betterment of Society (Teachers)

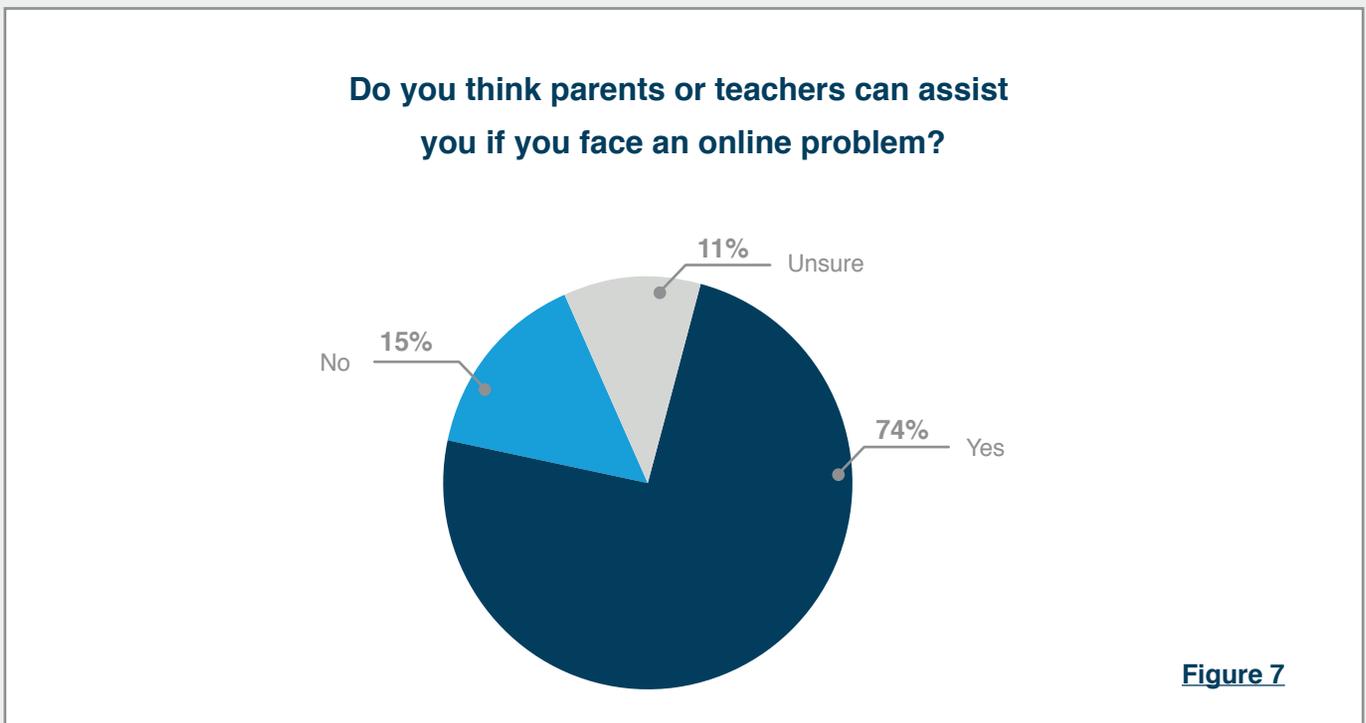
As stated above, cyber bullying takes place outside of the school setting, more so than traditional in-school bullying. Keeping this in mind, teachers around the world have created a fundamental way for students to continue their discussions and learning processes outside the classroom by giving them homework assignments that cover this. In doing so, students can be encouraged to think creatively about how to raise their own awareness about cyber bullying. Three students in the Robert Adams Middle School in Massachusetts (U.S.), for example, took part in a video sending a message about how cyber bullying, personally affects them in different ways.<sup>xix</sup> At the end of the video, they sent a powerful message about how words can hurt and, therefore, we should all be conscious to think about what we say.

Moreover, YouTube video blogging is already used as a medium to connect with policymakers and parents about how students are impacted by cyber bullying, but more importantly they also exemplify what they are learning. With such a huge audience, YouTube creates a great platform to encourage all adults to think about the evolution of bullying. A video can go viral and instantly ignite a social media campaign.<sup>xx</sup> These collective voices offer policymakers and parents' new ways of imparting knowledge to others about cyber bullying.



### 5- Offering Access to Guidance Counsellors for Children

Currently, minors have a sense of dishonour when talking to adults about problems involving their peers, particularly when it comes to being harassed online. Many choose not to raise these issues to their parents, teachers, or other socially responsible adults because of the potential fear of being perceived as "weak". According to our ICDL Summer Camp survey, over 26% of adolescents felt it was unlikely that a parent or teacher could assist if they are facing an online problem (See Figure 7).



**Figure 7**

Several youth choose not to bring up the fact that they have been (or are still being) cyber bullied, as there is a negative stigma of talking to parents about problems involving peers. Many people their age may perceive it as a sign of "weakness" because they need to rely on someone else to solve their problems. Confiding in a trustworthy, responsible adult who has the technical skills and the professional experience should be highly encouraged, because sharing a cyber bullying story is a strength, not a weakness.

Maintaining an open dialogue with someone who is more life-experienced can also help create a support circle that protects children and prevents their online experiences from worsening. Furthermore, our youths are seeking out help when it is needed, but they could play a courageous role in raising awareness of an issue that can help uplift other youths who face similar situations, thereby assuring them that they are not alone.

### **6- Addressing the Issues Directly with Your Child and Their Teachers (Parents)**

Playing a guardianship role, parents should be aware to address the topic of cyber bullying even if their child has not mentioned any problems or has not seen any form of it online. Chances are he/she has come across it and he/she might innocently be unaware of the issue. Even worse, the child may feel reserved to talk about it because they have seen it. On the other hand, parents may be unaware that it is their own child who is the perpetrator. Whereas no parent expects that their own child would take part in such actions, cyber bullying cannot take place without an instigator.

Fundamentally, staying involved in a child's life can help protect your child. Still, staying in constant communication, talking to them about using proper Internet etiquette (a.k.a. netiquette) and reinforcing family values is essential to a child's upbringing. Doing so will ultimately lead to a safer online experience, as it will help harmonise his/her life offline with his/her life online.

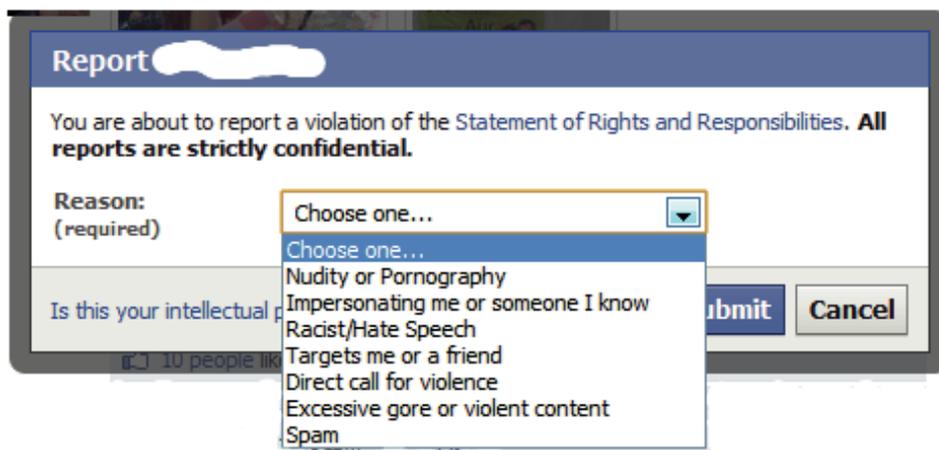
Maintaining an open relationship with teachers needs to be addressed, as well. Parents have the responsibility to know what their students are doing to tackle these issues and ensure that the school has a policy in place and that they're enforcing it effectively. Whether attending parent/teacher conferences, creating school assemblies, directly communicating with school faculty through email, parents who work in synergy with their child's school helps synchronise the messages and methods the child is following in school with what is being instilled in the home environment.

### **7- Staying Abreast with Social Media "Terms and Conditions" Policies (Parents)**

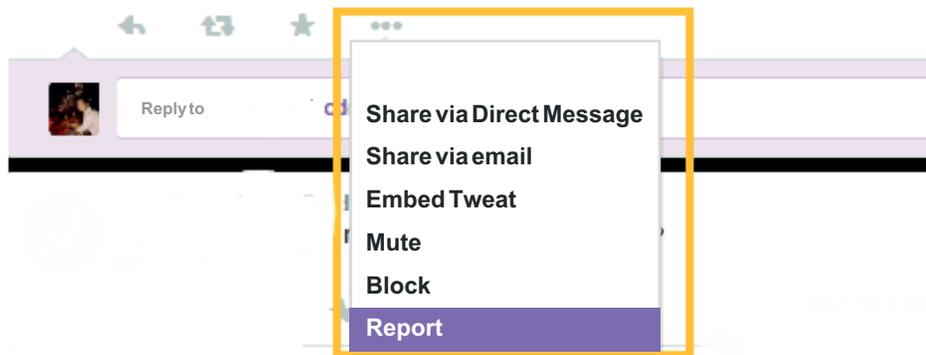
Parents must take the time to go through policy statements on social media websites.<sup>xxi,xxii,xxiii</sup> before their child creates a social media account. They need to make sure that they have a "no-tolerance" cyber bullying policy set in place, that there is evidence that they are taking immediate action and that it is a priority on their agenda. Most social media websites have an application embedded in every post, but very few (if any) of the main social media websites prioritise cyber bullying in a way to raise awareness.

Parents cannot rely solely on social media platforms to protect their children. Their algorithms for automatically detecting unwanted comments on a child's social media account with offensive comments simply does not track the different ways people bully. People's comments can be subtle with a clear intention of offending someone, which is why it is important to learn more about how to contact the appropriate social media authorities when a series of subliminally offensive comments occur.

### Facebook



### Twitter



### YouTube



### 8- Providing Access to Hotlines and Other Tools for Anonymous Victims and Good Samaritans (Government)

Even though targets of cyber bullying attacks have the ability to simply turn off technological devices and block offensive accounts on social media, the effects can still impact an individual once they see or know of a hurtful comment directed towards them. Multiple government entities need to collaboratively prepare themselves for the worst case scenario and be approachable for their citizens at any given time. It has been said that the harmful incidences of cyber bullying include words and images that promote suicidal thoughts and lead victims to consider committing suicide or other self-harming methods. More often than not, young people have become part of an Internet culture whereas such comments are not only accepted, but are also shared by people who have the similar intentions.<sup>xxiv</sup>

Several policymakers in the Western world had recognised that many young people do not reach out to an adult when they are being cyber bullied. It could be because they do not want to have their shameful incident widespread, or it could be that seeking help might be perceived as a sign of weakness. These countries have helped debunk these myths by reassuring children that going to an adult for help is a sign of bravery (not cowardice) and creating websites and hotlines for people who wish to talk about these urgent matters anonymously. Government officials have found that addressing the problem anonymously helps trigger conversations, as it ensures that the personal information a victim reveals is not going to be misused.

**BULLYING IS WRONG**

Whether it's physical. Or mental.

Do something about it. Tell your parents. Tell a teacher. Or contact the CyberBully Hotline. Your school's anonymous way to stop bullying.


**Call or Text 605.277.4026**

**CyberBullyHotline**  
Be Braver About It

### 9- Calling for Help with the Click of a Button

Desperate needs call for desperate measures and because the Arab World still lags behind on enhancing the public's cyber safety, it is important to provide resources that are quickly available and accessible to end users. Creating a cyber safety 'Help' button for those who have been violated gives Internet users (particularly children) the opportunity to taking charge of their own situation by relying on professionals who have experience in these fields.

Australian government entity CyberSmart<sup>xxv</sup> has implemented an application that anyone in the country can use as a centralised platform for matters around cyber bullying. This particular application offers counselling, reporting and educational resources (including people who converse with citizens one-on-one) for anyone who is facing an online problem. It is easily downloadable on any electronic device, including tablets and mobile phones and it can be installed on any of the four main web browsers: Explorer, Firefox, Google Chrome and Safari.



If such a feature and assistance is offered similarly in our region, it could be utilised from wherever the app is installed, including school networking systems, gaming centres and even home computers. Once the help button is installed, it can be accessed at any time for help or advice about something unsafe or upsetting that someone encounters while using the Internet.

## 🌐 CYBER EXPLOITATION: HOW IT STARTED



**Cyber exploitation is the act of misusing social media platforms, chat rooms or other means of information technology to manipulate an individual or deceptively utilise the individual's personal information for personal gain.**

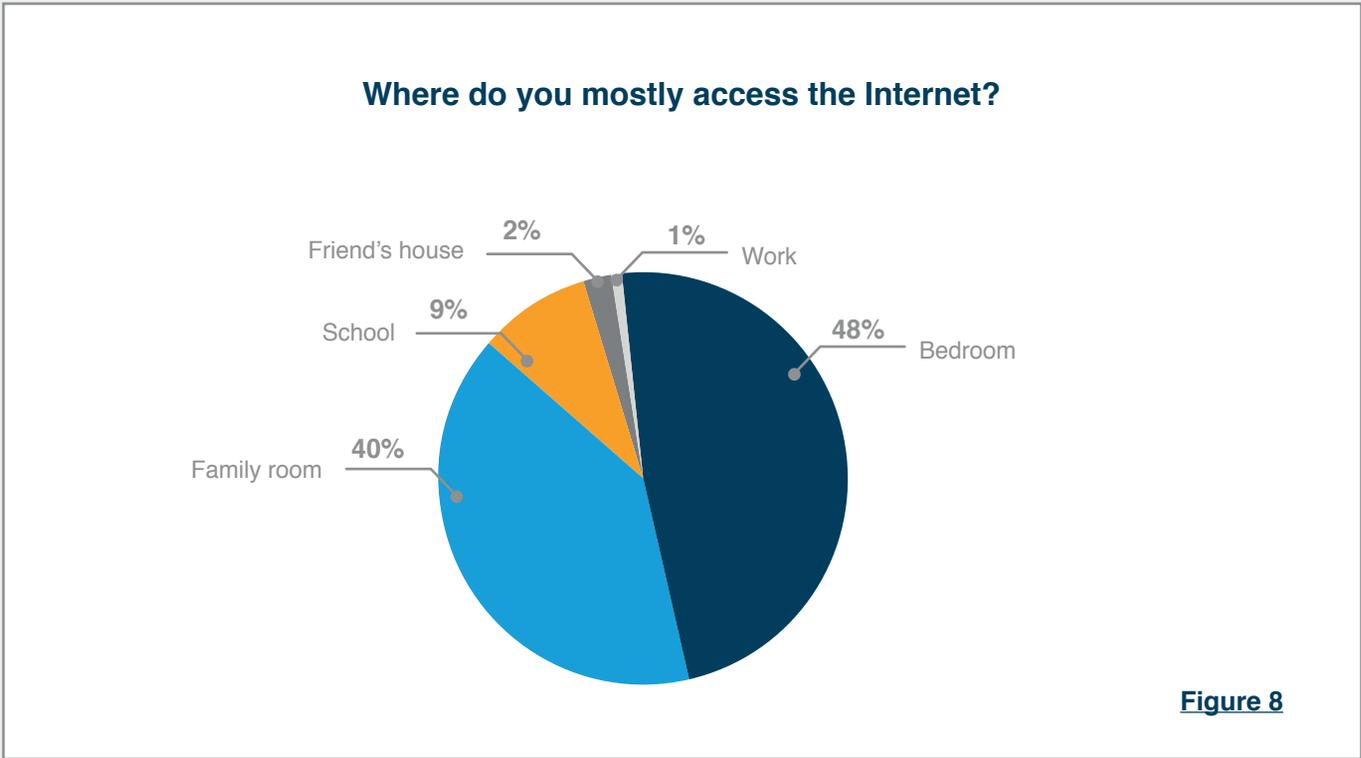
ICDL Arabia

When a parent takes a child to the cinema, which movies they allow them to watch? Based on film rating systematic standards, some movies may contain content inappropriate for under-aged children. Hypothetically, films with G ratings are allowed for children of all ages, PG suggests the need for "parental guidance," PG-13 implies that some material may be inappropriate for pre-teens and warns parents to be cautious, etc. Compare this to the Internet, where the vast majority of content is not blocked, where social media platforms provide no filters for what is allowable to be seen and where most content is accessed without adult supervision.

According to a 2014 study conducted by the Governance and Innovation Program at the Mohammed bin Rashid School of Government, over 44% of respondents believe that 14-year-olds indeed use their own electronic devices independently. Furthermore, a Microsoft study in 2013 concluded that 41% of parents allow their kids to use a gaming console unsupervised, 40% allow them unsupervised access to a computer and 29% allow their kids under age seven to use mobile apps unsupervised.

In our ICDL Arabia survey, nearly half (48%) of youth stated that they mostly access the Internet in the privacy of their bedroom (**See Figure 8**). In other words, they use the Internet with no adult supervision.

The fact of the matter is that it is irresponsible to be negligent of what children read and post on their social media accounts. Social networking eventually turned into a primary source for communication and keeping in touch with others for quite some time. That said, it is important to be conscious of what children post and - more importantly - how it can be used against them in the future. Initially, social media platforms were seen as outlets for people to control how they wanted to be perceived, which has resulted in posting information about themselves and sharing things that they consider entertaining or interesting. Consequently, this information can be misused by anyone if they have access to it.



#### 1- The Disparity between Parents and Children about Online Activity

According to the Family Online Safety Institute in the United States, a substantial gap exists between how teenagers think their parents monitor their online activities and their parents' reported oversight. In their 2012 survey, 39% of teens said their parents monitored their activities closely, compared to 84% of parents who were asked the same question. Later, both sets of individuals were asked if parents were well-informed about their online activities. 91% of parents believed they were at least somewhat informed about their child's online behaviour, while only 62% of teens agreed with that statement.

This is particularly relevant in a case that was exemplified in the beginning of the 2011 film, *Trust*.<sup>xxvi</sup> Annie, a 14-year-old girl, received a laptop as a birthday gift from her parents. She ends up meeting a stranger online who initially said he was 16 years old. As he continues to groom her, she begins to gain his trust and conceals this from her parents. At that point, this stranger who only pretended to be 16 now had more control over Annie's emotions than her own parents. The film highlights the ease by which an adult with bad intentions can totally control and manipulate a child.

Situations similar to these are constantly happening and the Middle East is certainly not an exception. To prevent these situations from happening, it is best for a parent to be conscious of what their child is doing online and to separate the child from a seclusive environment like a bedroom to a more common area, like the family room. Also, keep in mind that, contrary to what many online resources discuss, this does not just refer to keeping a laptop out of the bedroom. A child having a well-enabled cell phone gives that child the opportunity to use the Internet anywhere they go.

## 2- "Over-Sharing" Information: How Much is Too Much?

When someone logs onto their Facebook account, the profile has an "About" section available for users to fill out. When taking a close look at some of the questions being asked, users can recognise that they have the option to fill out some very personal information: everything from their birthday, to their hobbies, to their political views, to where they go/went to school, to the city in which they live. Facebook even gives people a space to add their phone number and their home address. This is just one of the many social networking sites that provide an arena for minors to potentially lose control of their private information.

Contrary to belief, posting any information online is open to be seen by anyone. Adjusting an account's privacy settings helps, but adding any information to a social media account immediately puts the person at risk of having that information stolen and misused. Additionally, sharing simple things like a favourite number or a nickname gives a hacker a better chance of guess your password and steal your identity.

**The ICDL Summer Camp Survey concludes that 16% of those surveyed have received online requests for private or personal information from a stranger.**

## 3- Location-Based Services

While some forms of cyber stalking can clearly invade children's privacy, other forms may not seem as explicit but can be just as harmful. In 2013, Digital Trends posted an article on the potential dangers of geotagging.<sup>xxvii</sup> It mentions how this has been a very popular tool used by the younger generation ever since it was created, particularly for when an individual posts a picture online. Although this feature may be used by people with the good intentions to connect with others in the same area, geolocation applications allow burglars with tracking software to find out when a person's home is empty. In fact, Gerald Friedland of the International Computer Science Institute conducted a survey in which 78% of ex-burglars strongly believed social media platforms are being used by current thieves to burglarise personal properties.



[www.ajacwebdesign.com/blog/3-ways-to-bring-together-social-media-and-local-seo](http://www.ajacwebdesign.com/blog/3-ways-to-bring-together-social-media-and-local-seo)

It is a feature that seems harmless on the surface because several social media platforms have incorporated it into their websites, including but not limited to Facebook, Twitter, Instagram, Foursquare and Flickr. That said, if a family member posts something online about how the family being out of the country on vacation, it can be seen by someone else as an opportunity to rob a home, giving them a specific time interval for when the person can break in without the fear of getting caught.<sup>xxviii</sup> This is especially important for when the geotag feature is not visible to a social media user: sometimes the applications are embedded through the settings of a smartphone. This, in turn, could compromise a child's privacy and safety if and when he/she ever posts an image online.

### ● CYBER EXPLOITATION: WHY IT IS A PROBLEM

Out of every concern mentioned in this report, online predators can probably cause the most harm to children. Unlike the previously mentioned problems, not only can online predators be a negative influence on a child's social life, but they can eventually do immense harm to them physically... even if they are not in direct contact with them.

Furthermore, the source of the problem (the perpetrators who get innocent youths to perform unwanted acts online) is enormous. The United Nations and the FBI estimated that 750,000 paedophiles are online at any given moment.<sup>xxix</sup> What makes matters worse is that many of these predators (almost all of them men) are not penalised or charged with any crime to receive any kind of punishment.

Any child in any corner of the world can be vulnerable to these predators, if they have Internet access and the ability to chat with unknown person unsupervised by a responsible adult. The key component is that it is in a private setting, because their lack of guidance leads to their exploitation. When a younger person expresses something online it reveals information that an online predator can use to establish a connection and gradually gain a child's trust and confidence.

Children in the Arab World are not immune to this, either.

**16% of survey respondents in the ICDL Summer Camp claimed that they have received inappropriate online content in the past.**

## 🕒 CYBER EXPLOITATION: RECOMMENDATIONS

### 1- Creating a National/Regional Online Predator Registry Website

In the United States, the Department of Justice (particularly the FBI) coordinates a series of agencies and websites, one for every state and territory, responsible for keeping a database of convicted felons. With the goal of educating the public and to prevent any further victimisation, each offender is individually classified so that people within that state know which threats in particular live in their area and why each person on that website is displayed for the world to see.

Typically, each state has three levels of offenders<sup>xxx</sup>. The hierarchy exists to determine who poses as bigger threats for future exploitation-related crimes. Level 1 offenders determines that the risk of a re-offense is low and the degree of danger posed to the public by that specific offender is not very high on the Department of Public Safety's priority list; Level 2 offenders are considered moderately dangerous and Level 3 offenders are considered extremely dangerous. Qatar's government has taken an institutional initiative of this, as well, as they have prescribed a jail term of up to 5 years in prison and a fine of up to 500,000 QAR for anyone who "produces, promotes, uses, imports, or distributes child exploitation materials."<sup>xxxi</sup> The UAE is moving forward on a plan to set up a sex offenders registry as it continues its first steps of establishing comprehensive child protection laws.<sup>xxxii</sup> and has introduced a number of laws: Federal Law 5 (2012) Article 17 to combat cybercrimes targeted at juveniles which are punishable by imprisonment for a period of at least one year and a fine not less than fifty thousand dirhams and Federal Law 5 (2012) Article 18 covers use of IT to acquire child exploitation materials shall be punished by imprisonment for a period of at least six months and a fine of not less than one hundred and fifty thousand dirhams and not in excess of one million dirhams.<sup>xxxiii</sup>

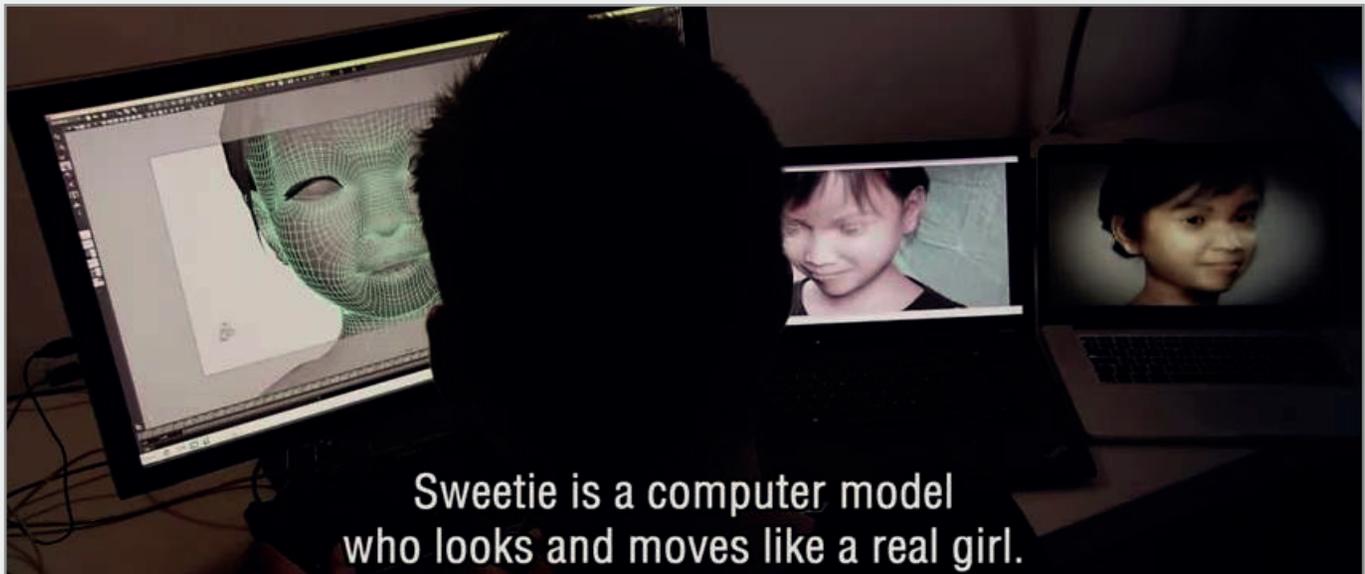
What each Arab government can do on a state or national level can also be done on a regional level. The MENA region is capable of working with each other in capturing online predators by sharing online information. Not only would this type of collaboration show that the region is serious about tackling the problem institutionally, but it would further unite the nation on a holistic level.

### 2- Case: A Robot Exposing Indecent Exposure

International child rights federation Terre des Hommes in Netherlands created an experiment in an effort to illustrate just how prevalent cyber exploitation has become. In 2013, they created a talking computerised mannequin that impersonates the looks, sounds and movements of a real girl. After doing this, they decided to use an application to test out how many predators would talk to her online. In the main video they uploaded, it showed just how problematic and prevalent these indecent acts were.<sup>xxxiv</sup>

While Sweetie is chatting, they track down the men. Terres des Hommes collects all this information (including video footage of men indecently exposing themselves) and they eventually handed over their personal information to Interpol (a cyber crime programme working to identify emerging threats to enable police to respond on an international level). In 10 weeks, they identified the first 1,000 predators, documenting cases from over 60 other countries, including 7 in the Arab World.

These robots can be created quite easily and can help keep the online world a safe environment for children.



### 3- Refer to Lists of Recommendations Provided by Online Resources

Websites like ThinkUKnow (supported by the Child Exploitation and Online Protection Centre in Great Britain) provide great tips for caretakers<sup>xxxv</sup> and children in both primary<sup>xxxvi</sup> and secondary school<sup>xxxvii</sup>. Since there is a page directed towards each target group, guardians can use this platform to review with their children.

The following are some of the subjects that the UK's **CEOP** (Child Exploitation and Online Protection Centre) covers in their videos:

#### ※ The Concept of "Friends":

Before social networking became an essential component of our social lives, almost all of the friends and connections were made through face-to-face interactions.

Online friends are very different than offline friends. Fundamentally, the younger generation has a new perception of what a friend is, due to the very language that social media platforms use. Many children enhance their social circles through meeting other people online who share a common interest. Examples include, but are not limited to, online gaming sites, online forums and online chat rooms. Each of these online entities contributes to society's transformation of how one can connect with others. Although it has made it easier for people to connect with others and although young people's idea of a "friend" might be very different than an adult's, they need to be aware that it is also much easier for an online predator to exploit a child's personal information and misuse it.

**Reflection questions to discuss with your child:** "What is a friend?" "What does a friend mean to you?" "Is your definition of a friend different from what it means to your child? If so, how?"

**Tip for Parents:** Advise your child to avoid adding or accepting requests from people they have not met in person.

**Reason:** Making someone a "friend" gives that person access to all the information you share. This does not just refer to what you post, but it also means that the person knows what you look like, where you live and any other interests you may have.

### ※ Think before you Post:

The importance for everyone to think before they share personal information has been widely recognised. It is easier said than done, as many people make use of the cameras on their phones by taking pictures of themselves (**also known as selfies**) along with videos of where they are and what they are doing. Immediately, many people upload this content onto social media networks like Instagram, Vine and SnapChat.

Once information is uploaded on the Internet, people can lose control of how the content is perceived. It is always best for a parent or caretaker to have a truthful and rational conversation with what their child is posting and why it could be dangerous. In addition, remind them to talk to their friends about not posting any content of them on their behalf. This refers to friends tagging your child in pictures that may not be appropriate for other people in their online community to see.

**Reflection questions to discuss with your child:** "What is your child's thought process for when he/she posts something?" "Would your child share the information they post online with people in an offline setting?" "Would they message or respond to someone they did not know about the content they posted?" "In what situations is it all right to post personal information?"

**Tip for Parents:** Encourage your child to think before uploading on the Internet, particularly what they are posting and to whom they are messaging.

**Reason:** Whatever is posted on the Internet stays on the Internet forever.

### ※ Do Not Give Strangers the Benefit of the Doubt:

As stated before, online identity is a very crucial component to a child's life. However, when anonymity is taken into account, the online identity of an innocent youngster can eventually be a very inadvertent component to their cyber exploitation. This is especially important to note when talking to your child about online predators, because not everyone is who they claim to be online. Take the previously mentioned film, *Trust*, for example. By using instant messaging, the online predator who exploited the 14-year-old girl used a picture of a young boy her age in an effort to get on her level and eventually lure her to him.

Parents should also be vigilant of hackers, as well, making sure that the social media networks their child is using are secure enough. Arenas such as MySpace and Snapchat, for instance, have been claimed by youth as popular platforms. Security experts have seriously questioned Snapchat's commitment to protecting its software.<sup>xxxviii</sup> Social networks can only do so much to protect children online, which is why it is important for parents to get involved directly with their child's social media accounts.

**Reflection questions to discuss with your child:** "Which social media networks does your child use?" "Would they message or respond to someone they did not know about content they posted?" "In what situations is it all right to post information?"

**Tip for Parents:** Know who your child is talking to on the Internet; don't be afraid to learn more about your child's social life.

**Reason:** Whatever is posted on the Internet stays on the Internet forever.

## CONCLUSION

The online world offers many opportunities for children of all ages to socialise and spend time on all kinds of interesting programmes. This has created several positive effects for everyone to experience and has brought us closer to information, along with family and friends. Nonetheless, it has also brought us closer to dangers that were, at one point in time, solely offline. Solicitation and digital exposure of under-aged children, identity theft, cyber bullying and cyber addiction are only some of the online aspects of which many adults stay negligent. These online risks have not only shifted to the online world, but they have magnified due to the Internet being a relatively new arena combined with its constant evolution.

In this report, ICDL has indicated the substantial risks that not only correlate with results from international studies, but also highlight the lack of regional research on the topic of cyber safety. With the lack of transparency on this issue, there is a desperate need to improve our methods of communication in an effort to prevent ongoing online risks. This particularly relates to what citizens (particularly young people) need to learn, why parents and teachers should help them develop skills and how governments should implement strong policies and widespread strategies to combat these cyber issues.

We leave you with three main messages to think about:

### **1- Just because you cannot find it does not mean it is not there**

When reflecting on all three presented issues, one of the main lessons to learn is how the Internet, although not malicious by nature, can become a portal for individuals to get into trouble if the right cyber safety measures are not put in place. The process can be so gradual that it is almost unnoticeable. A child relying on the Internet to occupy their time becomes normal. Making fun of someone online becomes the status quo, because everyone else is doing it. Chatting with a stranger is satisfying because, after months of talking, a child develops a connection and a secretive trust that no one else understands.

### **2) Be aware that an Internet experience is not "one-size-fits-all"**

Reiterating what was discussed in the final part of the cyber-bullying section, we need to understand that people are negatively impacted online in different ways. Each individual is different and therefore the solutions to these complicated problems cannot be painted with the same brush.

Additionally, different roles exist in perpetuating online culture, but it is always important to note that bystanders (i.e. people who are not directly affected by a cyber risk) have an important role to play in mitigating any cyber threat. People react to comments posted on social media in different ways. Nevertheless, it is always important to report any social media posts that were clearly intended to harass or offend someone and (if unsure) confide in someone who may have more knowledge on the subject.

### 3) This is an Evolutionary Thought Process

Subjects related to cyber safety are never static. As technology changes over time, so do people. Reflect on how most children in the GCC region use the Internet. A decade ago, the majority of us primarily used desktop and laptop computers to access the Internet. Fast-forwarding to now, we have seen youth quickly shift to phones and tablets. What happens a decade from now will be based on a variety of factors, but keeping in mind the evolution of technology is important for how we think about general safety issues and maintaining our awareness of those issues.

※ **Cyber addiction** does not just refer to how much we use the computer anymore; it is also about our total dependence on any Internet-accessible smartphones, tablets, game consoles, televisions and any other gadgets.

※ **Cyber bullying** can happen on any platform and so can cyber exploitation. Rules and regulations on cyber bullying need to be updated quicker as an increasing array of social, business and personal activities shift to the cyber world at a more rapid pace.

※ **Cyber exploitation** is a constantly changing issue as predators are finding innovative ways to solicit minors. Children are just as influenced by adults as they are face to face.

## CALL-TO-ACTION

A minor using the Internet without cyber **awareness** is guaranteed to suffer immense consequences. This is why it is essential for adults to stay conscious of what they are doing online. These problems are real on a grand scale and require the same degree of educational vigilance as other lifestyle risk categories such as sex, drugs and alcohol. Use preventive methods to manage and avoid the hazards children face by keeping up-to-date with new and relevant issues that arise on the Internet, making yourself **available** in a supportive way and staying **active** in their lives.

In doing so, we believe that governments, educators and parents should be at the forefront in preventing these cyber risks in children. As mentioned in the "Analysis" section, it is essential for us to work collectively and synchronously on these matters. That said, each stakeholder plays a different role, and based on their fundamental responsibilities, ICDL Arabia believes each player can focus on accomplishing certain goals within their areas of expertise.

### For governments:

- Invest in more cyber safety research to find out more about society's implications on Internet usage.
- Establish legal policies to protect citizens, both nationwide and regionally.
- Create and provide funding for organisations that attempt to empower victims exposed to cyber risks as well as rehabilitation programmes for those who have committed cyber crimes.
- Collaborate with different authorities within the government to provide the most useful and up-to-date information to apply the most effective techniques for teachers, parents, and youth.

### For teachers:

- Work with administrators to develop school policies and awareness programmes that cater to students and parents within the schooling system.
- Request for training on issues related to cyber safety.
- Create a constructive learning environment for students to interact with one another inside and outside the classrooms about cyber risks.
- Organise school assemblies and parent/teacher conferences to re-establish strong relationships with the students' parents.

### Parents/Guardians:

- Monitor your child's online usage by following the recommendations set by professionals in the areas of cyber safety.
- Guide your children into becoming responsible, ethical, and informed adults by being an active role model at home.
- Continue learning about the newest up-to-date technologies and applications your child might be using.
- Maintain an honest and open dialogue with your child about what they're doing online.

## ACKNOWLEDGMENTS

ICDL Arabia's annual report is a product of the efforts and commitments of the partners, sponsors, and students who supported and participated in the ICDL Summer Camp 2014. The compilation of the data was undertaken by ICDL Arabia and facilitated by Universities and training institutes that hosted ICDL Summer Camp 2014 across the UAE.

We are forever indebted to our partners and sponsors in ICDL Summer Camp 2014 for their ongoing monetary and in-kind support. The generous contributions made by visionary leaders, concerned government organisations and responsible corporate citizens were instrumental to enrolling over 400 students in a productive summer filled with learning new skills as well as recreational and social networking activities. Acknowledgment also goes to the ICDL Arabia team for gathering such valuable information and for putting this report together which will hopefully inspire qualification and educational regulators in their efforts to improve ICT skills and cyber safety awareness within our education system.

Partners, supporters, and sponsors of ICDL Arabia Summer Camp 2014 included:

- ✧ Abu Dhabi Education Council (ADEC)
- ✧ Abu Dhabi Systems & Information Centre (ADSIC)
- ✧ Abu Dhabi University
- ✧ Ajman University
- ✧ Atlantis Water Park
- ✧ Brother International
- ✧ Canon
- ✧ Centre of Excellence for Applied Research and Training
- ✧ Emirates NBD Bank
- ✧ HSBC Bank
- ✧ ITP Publishing Group
- ✧ Mashreq Bank
- ✧ National Institute for Vocational Education (NIVE)
- ✧ Nokia
- ✧ RAK Red Crescent
- ✧ Seawings
- ✧ Sharaf DG
- ✧ UAE Ministry of Interior – Child Protection Committee
- ✧ UAE University

Last, but not least, we want to acknowledge and thank you the reader for taking the time to read our report on such a prevalent and pertinent issue at this day and age. We hope you finished reading this document with a greater consciousness about the issue and the conscience to get actively involved in improving ICT skills and raising cyber safety awareness within our educational system and throughout society.

## REFERENCES

- i** The Kaiser Family Foundation defines "heavy media users" as those who spend 16+ hours on any type of media every day; this accounts for 21% of 8 to 18 year olds in the U.S. in 2010. "Moderate media users" are those who spend 3 to 15 hours per day on the Internet, and "light media users" are those who spend less than 3 hours per day. <http://files.eric.ed.gov/fulltext/ED527859.pdf>
- ii** Refer to Paul Poindexter, Sharon Meraz and Amy Schmitz Weiss's book: Women, Men, and News: Divided and Disconnected in the New Media Landscape (page 215) [https://books.google.ae/books?id=F\\_-OAgAAQBAJ&pg=PA215](https://books.google.ae/books?id=F_-OAgAAQBAJ&pg=PA215)
- iii** Refer to Women and Media in the Middle East: Power Through Self-expression (page 139) by Naomi Sakr <https://books.google.ae/books?id=BZ33AgAAQBAJ&pg=PA139>
- iv** 2013 Ofcom Report <http://media.ofcom.org.uk/news/2013/younger-children-turn-from-phones-to-tablets/>
- v** Symptoms of Internet Addiction <http://www.helpguide.org/articles/addiction/internet-and-computer-addiction.htm>
- vi** This is according to the journal Cyberspchology, Behavior and Social Networking, where they conducted a study from over 89,000 individuals in 31 countries. <http://www.techtimes.com/articles/22541/20141219/internet-addiction-affects-6-percent-of-global-population-study.htm>
- vii** Refer to page 758 in the following URL <http://online.liebertpub.com/doi/pdf/10.1089/cyber.2014.0317>
- viii** Blacklists and whitelists on SelfControl: <https://faithinformed.wordpress.com/2010/05/28/selfcontrol-for-those-without-self-control/>
- ix** National Crime Prevention Council's report on Cyber bullying: [http://www.ncpc.org/resources/files/pdf/bullying/cyber\\_bullying.pdf](http://www.ncpc.org/resources/files/pdf/bullying/cyber_bullying.pdf)
- x** Effects of Cyber Bullying (for Bullies): <http://www.stopbullying.gov/at-risk/effects/>
- xi** Child Trends on Bullying: <http://www.childtrends.org/?indicators=bullying>
- xii** School Bullying in the Arab World: A Review [http://www.academia.edu/6594541/School\\_bullying\\_in\\_the\\_Arab\\_world\\_A\\_Review](http://www.academia.edu/6594541/School_bullying_in_the_Arab_world_A_Review)
- xiii** Ditch the Label's Cyber Bullying survey (2013) <http://www.ditchthelabel.org/downloads/the-annual-cyber-bullying-survey-2013.pdf>
- xiv** Be Web Aware (Cyber bullying): [http://www.bewebaware.ca/english/cyber\\_bullying.html](http://www.bewebaware.ca/english/cyber_bullying.html)
- xv** UAE's laws on defamation:  
<http://www.tamimi.com/en/magazine/law-update/section-5/october-3/legal-risks-for-social-media-users-in-the-uae.html>
- xvi** Learn more about what the Departments of Education and Health in Australia are doing to fight cyber bullying in schools:  
<https://education.gov.au/bullying-research-projects>
- xvii** Digizen Cyber bullying Lesson Plan: [http://www.digizen.org/downloads/cyber\\_bullying\\_lesson.pdf](http://www.digizen.org/downloads/cyber_bullying_lesson.pdf)
- xviii** Common Sense Media Lesson Plan: [https://www.common Sense Media.org/educators/lesson/cyber\\_bullying-crossing-line-6-8](https://www.common Sense Media.org/educators/lesson/cyber_bullying-crossing-line-6-8)
- xix** Cyber bullying in Robert H. Adams Middle School <https://www.youtube.com/watch?v=Jz-HwnyvUwY>
- xx** Successful case studies on cyber bullying in Australia:  
<http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/teachcasestudy.aspx>
- xxi** Facebook bullying policy: <https://www.facebook.com/safety/bullying/teens/>
- xxii** Twitter bullying policy: <https://support.twitter.com/articles/15794-online-abuse>
- xxiii** YouTube bullying policy: <https://support.google.com/youtube/answer/2801920?hl=en>
- xxiv** The "Cyber Bullying Virus" video, which explains how thoughts shared on social media platforms can go viral in a matter of minutes, now has over 1.5 million views: [https://www.youtube.com/watch?v=-5PZ\\_Bh-M6o](https://www.youtube.com/watch?v=-5PZ_Bh-M6o)
- xxv** Learn more about CyberSmart: <http://www.cybersmart.gov.au/About%20Cybersmart.aspx>
- xxvi** Trailer for the 2011 film Trust: <https://www.youtube.com/watch?v=k9J3fBSpXwc>
- xxvii** Digital Trends: Geotagging  
<http://www.digitaltrends.com/photography/could-you-fall-victim-to-crime-simply-by-geotagging-location-info-to-your-photos/>
- xxviii** Adam Savage, the host of a popular American/Australian TV show, was robbed after innocently posting a photo saying, "Now it's off to work" [http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?\\_r=0](http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?_r=0)

**xxix** Terres des Hommes: 750,000 child predators at any given moment

<http://www.terredeshommes.org/wp-content/uploads/2013/11/PR-Webcam-Child-Sex-Tourism-TDH-NL-04.11.2013.pdf>

**xxx** Massachusetts, like many states in the U.S.A., classify online predators in three levels:

<http://www.mass.gov/eopss/crime-prev-personal-sfty/sex-offenders/levels-of-sex-offenders.html>

**xxxi** Qatar's punishments for cyber crimes, particularly on child exploitation materials and hacking:

<http://thepeninsulaqatar.com/news/qatar/300301/law-issued-to-combat-cybercrimes>

**xxxii** <http://www.thenational.ae/news/uae-news/sex-offenders-registry-gets-closer-in-uae>

**xxxiii** [http://ejustice.gov.ae/downloads/latest\\_laws/federal\\_decree\\_law\\_5\\_2012\\_en.pdf](http://ejustice.gov.ae/downloads/latest_laws/federal_decree_law_5_2012_en.pdf)

**xxxiv** Terre des Hommes created a robot in 2013 that caught 1,000 child predators in 6 weeks; their video went viral in a matter of days: <https://www.youtube.com/watch?v=aGmKmVvCzkw>

**xxxv** ThinkUKnow for Caretakers/Parents: <https://www.thinkuknow.co.uk/parents/parentsguide/>

**xxxvi** ThinkUKnow for Kids in Primary Education: <https://www.thinkuknow.co.uk/parents/Primary/>

**xxxvii** ThinkUKnow for Kids in Secondary Education: <https://www.thinkuknow.co.uk/parents/Secondary/>

**xxxviii** 2014 article: "Snapchat isn't private" <http://money.cnn.com/2014/10/10/technology/mobile/snapchat-not-private/>