Masters Project Final Report

December 2017

Project Title	Cyber Safety Course for Middle School Children of the Asian International School		
Student Name	Nilma.A Weerasinghe		
Registration No. & Index No.	MIT/2014/070 14550702		
Supervisor's Name	Prof. K.P Hewagamage		
Please Circle the appropriate	**Masters Program**	**Type**	
	MIT-eLearning	**Research**	**Implementation**

For Office Use ONLY		

Cyber Safety Course for Middle School Children of the Asian International School

N.A WEERASINGHE
2017

Cyber Safety Course for Middle School Children of the Asian International School

A dissertation submitted for the Degree of Master of Information Technology - eLearning

N.A WEERASINGHE
University of Colombo School of Computing
2017

Declaration

The thesis is my original work and has not been submitted previously for a degree at this or any other university/institute.

To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Student Name: Nilma. A Weerasinghe

Registration Number: MIT/2014/070

Index Number: 14550702

_____

Signature: Date:

This is to certify that this thesis is based on the work of Mr/Ms. Nilma. A Weerasinghe

under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified Supervisor Name: Prof. K.P Hewagamage

_____

Signature: Date:

Abstract

In today's world more avenues are open for adolescents to engage in social communication and experiment with the risky behaviours of the Internet. Most schools are receiving Internet Safety education (ISE) in most part of the world. Unfortunately, still the Sri Lankan schools are lagging behind with the problems such as Cyber bullying, Digital Addiction, etc.

Three hundred students, with a mean age of 12 years, were recruited from the school. Findings from this study indicate that of a total sample of 300 middle-school students, a small grouping 75% are using the Internet and digital devices limitlessly and 12% beginning risky online communication behaviours with strangers. Students who communicated online with strangers were older and had higher rates of posting personal information and risky online behaviours. Majority of them (60%) seems to be using social network such as Whats App, which result in incidents such as Cyber bullying.

The Cyber Safety e learning course in aid of creating awareness for the Middle School students of the Asian International School was developed.

The online course was developed including different types of software to provide a variation of the content to the learner. Articulate Storyline, Adobe Captivate, Adobe premier, Moodle were used as technologies in developing the course. As the course is designed for the Middle school children, a pedagogical approach was implemented.

The course was designed with conditional navigation, where the children are not allowed to move to the next activity unless completed. Activity completion will also be indicated in the lesson modules for the learners to know what they have successfully completed. Further, marks allocation has not been focused strictly as the prime Goal of this project is to increase the awareness of Cyber Safety. Further, learners can always repeat the lessons as the course flows in a spiral method. The menus are not included in the lessons as the audience is young learners and they may be distracted easily. Motivational reward badges are entitled for quizzes to promote interest in following the course.

The Cyber Safety course is implemented in the school for Middle School children for two hours weekly afterschool. Each batch consist about ten students. The course is allocated for three months in the Second Term.

Keywords: Internet Safety Education Digital Addiction Cyber bullying Middle School Children.

Acknowledgments

I would like to take this opportunity to pay my sincere gratitude and respect who helped me in numerous ways throughout this project. First and foremost I would like to pay my sincere thanks to my project supervisor Professor K.P Hewagamage for the valuable guidance and support given. Also, I'm grateful to our project coordinator Dr.Thushani Weerasinghe, who understood the troubled situations and guided throughout the success of the project. Not forgetting my teachers of e learning module Ms.Nisha Kariyawasam, Mr.Hakeem Usoof and Prof. Gihan Wickramanayake.

Further, I'm also grateful for the people who provided great assistance in succeeding the project. I'm grateful to Ms.Suven Thambar, Head of the Middle School of the Asian International School for initiating the project topic for me. Also Mr. Razmy Zahir the Head of the Computer Department and Mr. Jerome Francis Lab Administrator of the school and the teachers of the staff by helping me to conduct surveys, testing and evaluations.

Last but not least, I'm thankful for my parents and my husband for supporting me all along in succeeding the project.

Thank you!

Contents

List of Tables

List of Figures

List of Acronyms

ICT – Information and Communication Technology

Moodle –Modular Object Oriented Dynamic Learning Environment

SCORM – Sharable Content Object Reference Model

ADDIE- Analysis-Design-Develop-Implement and Evaluate

Chapter 1: Introduction to Cyber Safety Issues

1.1 Introduction

Technology and the Internet has paved its ways to open new avenues for the people in Financial, Marketing, business, Medical, etc. e-commerce has ease the purchasing and delivering process, while smart phones and tablet devices have captured people's attraction with their easy accessibility to do daily processes.

Social networking has made it very simple for the people around the world to communicate and interact with each other. Different age groups can interact within seconds through any hand on digital device as a result of the Internet.

Moreover, the importance of using technology and the Internet in the realm of education is identified. The students can be beneficial in many ways through the use of the Internet, such as online academic support, e-tutoring in schools.

As the developed online course is focused for the middle school students, it can be outlined that technology and Internet has a helping hand for the academic support as well as personal development. For an instance, rather than merely reading a textbook to understand the concepts, a web based unit with animation and videos may be fruitful to develop the cognitive skills for a better understanding.

However, technology and Internet could also be dangerous as such with the misuse of technology. Children could be probe to any misuse or online threat on the Internet. As they are in a very sensitive age, they can be often affected negatively. Further, there is a potentiality that online environment could harm the children not only in the school but also at home. To name such threats, paedophiles who are looking for inappropriate connections with the children and child pornography seekers.

An Australian child safety website 'Kids Matter' indicates that 95% of children as young as 8-11 years have access to the Internet and that 45% of this same age group use social networking sites. Similarly an American child safety website, 'Guard Child' indicates that 65% of 8-14 year olds have been involved in cyber bullying and that as much as 90% of 8-16

year olds have seen online pornography! These statistics are corroborated by many other sources of child cyber safety statistics in the West and in some parts of the Eastern world.

High risks of fake profiles are recorded in the past decades in Sri Lanka as well [Table 1] which has resulted in harming the reputation of the well being of the children. In contrast to the social interaction development that is cultivated through apps and social networks, there is a high tendency that the children could be easily exploit and cause harm to other students. Cyber bullying is one such harassment that has emerged with the peers through the use of technology. Another threat that could be outlined for the middle school children are the spreading of personal information online. Thus, I believe a constructive solution to overcome the above mentioned problems can be an interactive online awareness course that would enhance the understanding and responsibility of the middle school children on how to use the online in a safe manner. If students are educated properly about the online threats, ethics and digital laws, the risks that could affect them could be minimized. On the other hand the children who are without proper awareness might unnecessarily fall in to danger pits and wrong hands.

1.2 The Context

This thesis is focused in bringing out an instructional design solution for the middle school students of Asian International School, Colombo. The Asian International School, Colombo trains students for the Edexcel examinations of the U.K. The school conducts ICT curriculum from primary to Advance Level under the guidance of the British Council of Sri Lanka.

The students of the Asian International School are a hub for discovering new technology and expanding knowledge through the use of the Internet. According to the survey findings [1] 90% of students access the Internet through their smart phones or Tablet devices. The school too exposes children to many avenues of academic streams through Internet for a better performance of grades. More, specifically technology brings many benefits for middle school students, as the abstract concepts of subjects can be visualize for a better understanding and students are more likely to understand topics through a web based inquiry unit which includes visualization.

Majority of students stated that they use their smart phones or other digital devices for online games and some of them are severely addicted to playing online games and social networks. As a result, there seems to be a progress in the ill-behaviour among the students. Many of the students are being given cautionary warnings and suspensions due to lack of concentration,

indecent acts in the class and hyperactive behaviours, which is suspected due to the addiction to online games which activates hyper psyche and violence.

Thus, a proposed online course could effectively engage the all the students in the awareness course.

1.2.1 Vision

The vision is to facilitate the learners of the Middle school with a set of guidelines on Cyber Safety for creating social awareness among themselves. The traditional classroom teaching will not be ideal as it's not a compulsory subject for them to learn and it is a compilation of advices to follow. The children need to be given the learning in a playful, interactive and a creative environment. Such as, by attending discussion forums, chat sessions and sharing tools to collaborate their ideas with the peers. Movies and videos should be included for the children to interact and understand the risks behind several types of dangers with contact to Cyber. Creative activities with familiar tools for the children such as Power Point or movie maker should be given for them to be constructive on what they are learning. Also they can predict solutions to the given scenarios with related to different types of dangers. Further, facing to situations and making decisions will guide them in their real life as they walk through the Cyber world. Children will be totally in an online environment, where they follow the Demo videos and facilitator instructions to do the activities. Facilitator contact details and its policy procedures will also be included in the course.

Assessments are basically creative, innovative and fun loving exercises. A very few tests are included and mostly quizzes should be added as the objective of this course is to create awareness rather than increasing the pass rate. By delivering the important guidelines and resource of advices in a playful environment, students will be able to experientially learn the importance of safeguarding themselves from cyber dangers and learn to respectfully communicate through online.

1.2.2 Mission

In order to achieve the vision, the mission would be an e learning program. Online learning materials such as games, videos, audio can be provided for the learners to improve their skills in an enjoyable way.

When identifying the requirements needed for the institution to introduce such a new system, the main requirement is the technology. The administrative resources, maintenance of the devices, apps installation and cost on sound devices, networks should be highly considered.

Therefore, In order to implement such a system, financial readiness, infrastructure readiness, readiness of the students of using them and readiness of the staff has to be considered.

1.3 The Motivation

The main reason behind developing an e learning course is the author's interest in the field. At present the Internet and digital devices has become a part of everyone's life as stated in the introduction. Especially children of 11 to 16 years of age are mislead or misguided by the impact of the advancement of the technology. Providing an online course will offer the opportunity to support the diverse learner styles at the same time unlike face to face teaching.

There are many online courses offering cyber safety issues but those courses need initial registration for the courses as well as not authenticating for the need required. Further, the school needs an awareness course for different types of modules, such as Cyber bullying, pornography, information privacy etc, and the author has developed a new syllabus under required needs.

Further, the following problems lying in the existing school environment paved the way to developing an online course:

- Students with the use of "What's App" and indiscipline verbal behavior
- The students are not being taught of any safety methods or risk encounters of the Cyber world
- Majority of students stated that they use their smart phones or other digital devices for online games and some of them are severely addicted to playing online games and social networks.
- Cyber bullying has become another main issue in the school which has resultant to keep a halt mark in their school carrier.

Thus, suggesting a free online course with the ICT curriculum for creating awareness on cyber safety issues would be an ideal choice compared to face to face workshops, courses or highly paid irrelevant online courses.

1.4 Goal and Objectives of the project

This project is intended mainly to create awareness among the students about the learning of the ICT in a safe and secured manner. Our students today belong to society who is constantly connected to each other through digital media. The high exposure to the internet poses a danger to our students as it can lead them to undesirable content which may corrupt their value systems, and to unnecessary hurts. Thus, it is obvious that there is a problem.

The final outcome of the solution should be to equip students with life time social value competencies so that they can become secured, respectful and responsible users of Information and Communication Technology.

1.4.1 Goals

Mitigate the unhealthy behaviour of the Middle school students with the use of digital devices by introducing a virtual learning system.

1.4.2 Objectives
The project aimed to:

- develop an adaptive online learning environment based on their level of knowledge within one year.
- develop a standard curriculum which supports the learners to arouse or increase the awareness on the risks and threats of the online environment.
- promote learner motivation by introducing interactive activities and reward schemes such as, badges /certificates.

1.5 Scope

The course will specifically focus on:

- E-Learning web portal developed by Moodle as it is an open source software and based on a Learning Management System.

- This will help users to learn via web- Perform demos, Perform related activities online and experience real E-learning features.

- E-learning course will be driven by pedagogy rather than technology. The syllabus will be designed under three categories according to three age groups (11-16 years) which range from simple to complex. The teaching pedagogy will deliver the student as an experiential and accidental based learning in a creative and a playful environment.

- The system will enable free user registration and once the user is registered the user will be offered the correct level to follow the course based on the age group

- Teacher sign up is also available as learners are teenagers they needed to be guided up to an extent- facilitating them with discussion forums, chat

- For teaching method -video tutorials, Narrator, Audio clips, Images, online games, demos, Activities

- Motivation on self learning- Forum and chat locations

- Reward badges or stars at the end of game based activities

- Reward system- Producing a digital certificate at the completion of the course

- Real-time feedback- Each module contain a short activity about the learned content where the summary of results are displayed at the end of the completion of each lesson

- Module quizzes will be designed as impromptu quizzes in an enjoyable environment- the child may eventually get the grading by playing a game or matching a puzzle etc.

1.6 Deliverables and Outcomes

A Web based E-learning Portal will be developed in Moodle with below functionalities,

- User Registration and Profiling
- User based Learning (Customizable learning support depends on the user's requirement)
- User friendly Navigation throughout the course flow
- Online learning and activities
- Grading and assessment and feedback mechanism
- Online Help support / Forum / Help Menu/chat
- Rewards

Documents

- Interim Report
- Syllabus
- Course Maps
- Story Boards
- Instructional Design plan document
- Technical documentation
- User documentation
- Final report
-

1.7 Feasibility Study

1.7.1 Technical Feasibility

In order to develop LMS the technical knowledge and technical environment needs to be developed. They are as follows:

- Knowledge to develop and setup course in Moodle LMS environment

- Knowledge of tools to create course content such as, videos, animations, games, interactive work materials
- Knowledge to create SCORM packages
- Compatible development hardware to run Moodle and other necessary tools such as videos and games
- Compatible servers and Networks to host Moodle

- A Network admin is available for the maintenance and installation of the systems therefore configuring server networks can be processed with the available resources.
- The staff could be trained by me as I am a teacher of the ICT department using the LMS.
- The students can be made ready to accept the system as the course is inculcated to the ICT syllabus and the students will be ready to use the system by conducting an orientation.
- To develop the knowledge on Moodle and other tools, resources are available to download for free and other knowledge can be gained through you tube videos, tutorials and workshops. The school has the possibility to provide the intranet server and network facility to host Moodle. Developing cyber safety awareness course in the ICT curriculum is Technically Feasible.

Therefore, developing cyber safety awareness course in the ICT curriculum is Technically Feasible.

1.7.2 Social Feasibility

By introducing an e learning course the school can improve their status of reputation as the children will be benefitted with an additional knowledge apart from their curriculum. Further, as the children become aware on the risks parents can rely on their child safety in the school and in turn would be a beneficiary for the school when seeking new admissions.

As the child will have the access to report any online crime that he/she has to face through the use of the course, the school can assure the child's digital safety which can make the children a holistic citizen in the future.

As per the above mentioned factors the author has received accreditation by the Head of the Middle School to select the target group as three Grades in the Middle School; Form1, Form 2

and Form 3 to develop the e learning material. However, the said e learning course has to meet the standards of the School culture and protect the ethics of the target group.

Further the author also had to take up the challenge of the teachers of the staff who are resisting initiating this programme in the school due to unfamiliarity and increasing work load.

1.7.3 Economic Feasibility

The resources need to allocate for the system includes, software, hardware, infrastructure and effort.

The cost for the project as follows:

Resources	Amount(LKR)
Software(Moodle and free online tools)	**0.00**
Hardware(uses the available hardware resources)	**0.00**
Infrastructure (Internet, Electricity….)	**35000.00**
Effort for 200 man hours	**90000.00**

Table 1.1 Economic Feasibility

Thus, charges for the infrastructure is the only expenditure this system is feasible.

1.8 Dissertation Outline

Here in chapter 01, it is being described about the introduction of the project ": Cyber Safety Course for Middle School Children". In chapter 02, the background information of the project is described, providing others approaches to solve the problem. Chapter 03 describes the analysis phase of the project with the analysis concepts used. Chapter 04 provides a detailed explanation about the project design. Project development and implementation describes the 05th Chapter. Chapter 06 describes evaluation and results discussion is described in Chapter 7. Chapter 8 describes future work along with the conclusion of the project. References are stated at the end of the dissertation which is followed by the appendix and the list of figures, tables and abbreviations.

Chapter 2: Background

The background analysis will primarily focus on various learning theories and design models which are already available, followed by an evaluation of those solutions to find if there is already a suitable and applicable solution. Also describes the literature review to discuss the similar online courses and design considerations.

2.1 Literature Review

This section discusses researches and course developer's efforts in teaching students about how to be safe on the Cyberspace. Although all these researches and courses are directly not addressed to the specific middle aged group students, it is essential to study these in order to find a constructive instructional solution.

1. Dowdell [4] states that more adolescents are using the Internet for social communication and a source of information to experiment with risky online behaviors. In her study she outlines the risky online behaviors and describes online relationships with strangers middle school students are interacting with.

2. Robert Lucas [5] states "There is an old Chinese proverb that reads: "*Give a man a fish and you feed him for a day. Teach a man to fish and you feed him for a lifetime.*" The concept is the same here. Blocking and restricting websites doesn't do anything good for students in the long run, but teaching them how to be safe online enables them to practice good habits for their entire life. "

3. It has become an essential factor to develop and introduce e learning course on cyber safety for schools as children have the higher potentiality to fall into cyber crimes and threats round the world. In Sri Lanka too many children are victimized to crimes in social networking, etc. If the awareness starts from schools, a solid foundation to preventing such crimes could be resulted in future.

As the CERT records depict there has been a rapid growth in the cyber crimes from 2009 to today; **[Table 1-Appendix G]**

Thus proves the essentiality of proper awareness on Cyber Safety issues. The national CERT|CC (Computer Emergency Readiness Team | Co-ordination Centre) acts as the focal point for Cyber security for a nation. It is the single trusted source of advice about the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation, in responding to and recovering from Cyber attacks. CERT of Sri Lanka will act as a complaint handling authority for Cyber Crimes and Cyber complaints. The Sri Lankan citizens will get the opportunity to carry out their allegations to CERT online/offline.

4. Also the National Child Protection Authority of Sri Lanka states: [see Appendix G]

   "We are now working with the Ministry of Education, UNICEF, Microsoft, the Ministry of Justice, Sri Lanka CERT, ICTA Sri Lanka, the Department of Police, several private sector organizations, NGOs and INGOs to develop this module for using in schools. We do not want to discourage children from using the internet but we want them to be safe online,"

   That the country is in need of a curriculum in the school syllabus related to Cyber safety issues. The following statistic of CERT also discovers that more of the incidents have occurred due to the rapid increase of online usage and lack of knowledge on the online threats.

   "Senior Information Security Engineer of the CERT, Roshan Chandragupta said that 900 incidents related to cyber offences have been reported to Sri Lanka CERT|CC in 2015 from January till end of May. He added that in 2014 there were 2250 reported incidents of that nature – in 2013, 1200 and in 2012, 1100 were reported. He explained that over the years, the number of Internet users too has increased."

5. "We have received over 1,000 complaints against Facebook. We advise Facebook users to complain to the U.S. Company if they feel their privacy has been violated. If Facebook does not respond then we will investigate," Rohana Palliyaguru, senior information security engineer of the Sri Lanka Computer Emergency Response unit told Xinhua. [see 8]

"The agency has been receiving complaints of people hacking into profiles of young girls and changing their status, taking their pictures and creating fake profiles and threatening users for ransom."

The Colombo City Life News also recorded that at least 100 cases where schoolchildren were sexually abused or defamed via internet.

" Facebook accounts have been reported to the Cyber Crime Division of the Criminal Investigations Department (CID) during the past month", a senior Police officer said [see 15].

2.2   Review of similar systems

Numbers of online courses were identified on the Internet related to Cyber safety, which was developed in the UK, Australia and Newzeland. All these online courses are designed based on their requirement on creating awareness on cyber safety issues in their contexts. All the courses are interactively designed focusing the school children which have expected a positive outcome.

1.   An online challenge group organization in Newzeland [12].

"NetSafe's 'Learn, Guide, Protect', model was originally developed for schools to provide a framework in order to structure theirs. However, it is broadly application to anyone engaged in supporting young people develop safe and responsible online behaviours. It has three components: Learn, guide, protect."

2.   Safe Online Surfing [10]

""FBI-SOS is a fun, free, and effective way to teach kids how to use the Internet safely and responsibly," says Scott McMillion, head of the unit that manages the program in the FBI's Criminal Investigative Division." This course addresses the learner experience in a highly interactive manner, which provides children a game based learning experience.

3. Interactive video based learning

Figure 2.1 Interactive video based learning

Interactive video based learning (Figure 2.1) is a very good Instructional design solution but the course is not on free access. [13]

4. Australian government –office of the children's e-safety commissioner

Figure 2.2 *Australian government –office of the children's e-safety commissioner*

Australian government- office of the children's e-safety commissioner (Figure 2.2) is designed to help the children of Australia have safe and positive experience online and encourage behavioral change. The course is well adhere to children as well as adults; however the authenticity of the course to local setting cannot be achieved. Also the content of the course lacks interactivity for the learner as instructional strategies used

for the learner to discover information is not provided, such as instructional games and quizzes. [11]

5. NetSmartz

Figure 2.3 Netsmartz

This Netsmartz (Figure 2.3) offer number of presentations and video and tip sheets for different levels of grades. It provides information for parents, students. They provide interactive information and life stories for the children to learn the risks of cyber in real life but this information do not provide how to avoid them. Also the quizzes to assess the knowledge of them are not available. [12]

6. Syllabus designed by the CERT and NCPA of Sri Lanka(Course designed is under process)

   These syllabus criteria's are way too advanced for the school children and most of its topics are based on information security, whereas the proposed online course needs to cover from basic understanding of e safety to advance personal safety in the cyberspace.

   - Need for Information security
   - Information Security trends and Directions
   - Information Security and Methodology

- Basic Security guidelines and Best Practices when using Internet connected devices
- Protection of privacy
- Secure use of Social Media
- Incident handling
- Laws related to Information Security and Privacy in Sri Lanka
- Psychological impact and counseling

However, based on the research that I have made several different assumptions can be made in my project such as:

- The learners of the system should have the basic knowledge to use an online system
- The assessments will reflect the knowledge and the awareness that learner possesses from following the course.
- The facilities needed to implement the system are available in the school environment.
- Any school child with the basic knowledge of IT should be able to follow the course and get awareness.

2.3 Learning theories used in developing the course

Different types of theories are used to develop an online course. These theories deal with different aspects in time to time.

Theories based for instructional design are mainly categorized as, behaviourism, cognitive, constructivism.

2.3.1 Behaviourism

It is believed that the learning takes place primarily through the reinforcement of desired responses. Learners respond to each step by answering a question or completing a sentence.

2.3.2 Cognitivism

It is based on the principle that learning occurs through exposure to logically presented information. Eg: problem solving and comprehension

2.3.3 Constructivism

It focuses on how learners internalize what they have learned. Learner's construct knowledge from accommodation whereas constructivist focus on the individual learner.

The proposed system is designed for the school children for the age group ranging from 12 to 16 years, which requires pedagogy of behaviourism and constructivism. Children should be reinforce when learning takes place because autonomous motivation does not happen at this stage, therefore behaviourism principle has to be followed when designing the course.

Constructivism theory can be applied to designing the proposed course as it centralizes the learner in the learning process where, the instructor becomes only a facilitator. Therefore, in an online learning environment the learner will receive information through senses and created its own knowledge.

2.3.4 Dale's cone of experience

Dale's cone of experience is a commonly used theory related to instructional design and learning process. This shows the progression of the experiences from the most concrete to the

most abstract. According to Dale's cone the most concrete will be included at the bottom and most abstract will be on the top. Direct experiences or real life experiences are the concrete knowledge which is right at the bottom. Such as direct experiences (real life experiences) or interactive models. Direct experiences mean the experience which represents the reality, the closest thing to real life, everyday life. The theory states that a learner by merely listening or reading has a less tendency to absorb as it only awakens your senses. However, reading and listening plays an important role in the process of learning.

It has revealed that "action learning" techniques result in up to 90% retention. People learn best when they use perceptual learning styles. According to ("Dale",1969), instructors should design instructional activities that build upon more real life experience.
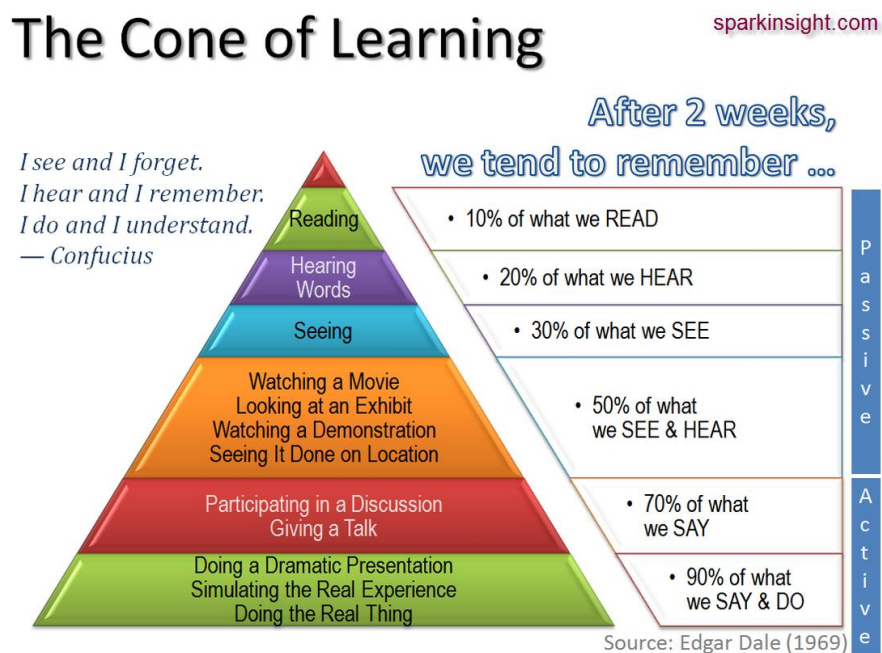
Figure 2.4 The cone of learning

The diagram above depicts how much an average student can retain, out of what it's learnt, through different channels of knowledge input. Learning outcome will totally depend on the capacity, concentration, absorption and imagination of the student.

Dale's cone of experience assures a 90% of learning outcome of what one actually does. And on the other hand a 10% of poor level is guaranteed in reading the material. The fact behind this is that when someone is reading a 100% of distraction of the mind involves since, learners

are possessed with different learner styles, since mind has to focus only reading. Whereas, Dale shows that 50% of what we see and hear and 70% of what we say is absorbed.

Thus, the proposed online course will be designed for school children, it is more appropriate to have animated based videos and interactive work material incorporated with real life activities. Thus, by adopting Dale cone's theorem each module will contain activities ranging from abstract to concrete. Eg: Learners 'will be able to understand the importance of learning cyber bullying through a lecture note, through visual aids, demonstration video, handout to download, practical hands on experience to make them design or capture their own audio/video clip on their own experiences or what they go to know of cyber bullying.

2.3.5 Bloom's Taxonomy

When developing an e learning course an important aspect to consider is how to satisfy learners with different level of knowledge. Bloom's Taxonomy therefore allows the Instructional designer to satisfy learner with more organized level of expertise. It is also called Bloom's Taxonomy of educational objectives.

Benjamin Bloom identified three learning domains: cognitive- mental skills, psychomotor-physical skills affective- growth in feelings or emotional areas. Instructional designers, trainers, and educators often refer to these three categories as KSA (Knowledge [cognitive], Skills [psychomotor], and Attitudes [affective]). This taxonomy of learning behaviours may be thought of as "the goals of the learning process." That is, after a learning episode, the learner should have acquired a new skill, knowledge, and/or attitude. There are six major categories of cognitive and processes, starting from the simplest to the most complex. Such as,

- Knowledge
- Comprehension
- Application
- Analysis

The cognitive domain of Bloom's Taxonomy can be revealed as,

- Remembering- recall or retrieve previously learned information

- Understanding- comprehending the meaning, translation and interpretation of instructions and problems
- Applying- use a concept in a new situation
- Analyzing-separate materials into component parts in order to understand the organizational structure

In order to design an online course a systematic development of instructional materials using learning theories are used. The key benefits of using an ISD model when designing courses include focusing efforts, getting quick results, lower down the costs and ensuring effectiveness of training. Various types of ISD models can be used to design this course. One of the most commonly used model is ADDIE.

2.3 Instructional System Design (ISD) Model

ADDIE model

It is an Instructional system design model. The process that most instructional designers use is called ADDIE. It contains five stages. Such as,

A-analyze
D-Design
D-Development
I-Implement
E-Evaluate

Analysis phase- In this phase, instructional problem is clarified and learning objectives are established. During this phase, the learning environment and learner's existing knowledge and skills are also identified. Framing the problem, gather data, determine resources needed, etc are some of them. During this phase the following questions should be addressed:

- Who is the audience?
- What are the new behavioral outcomes?
- What are the learning constraints?
- What are the delivery options?
- What is the timeline for project completion?

Design phase

The design phase includes learning objectives, assessments, exercises, content, subject matter analysis, lesson planning, etc. in this phase, creation of the lesson prototype, graphic design principles, design of the user interface.

Development phase

In this phase, the instructional designers put together everything they created in the design phase. At this stage the designers review the design based on the feedback.

Implementation phase

The actual presentation of the course is done at this stage.

Evaluation phase

The evaluation phase typically has two parts: summative and formative. In each stage of the ADDIE model formative evaluation is done. Summative evaluation is done for the test designed specifically for the content.

It was decided to use the ADDIE model in developing the prepared course. It is expected that number of resources in the Internet in addition to the course material would be a helping hand to accomplish this online course successfully.

2.3.1 ADDIE model for the proposed course

According to the ADDIE model the proposed course would be processed in the following manner:

Analysis Phase

During the analysis phase the requirements needed to create the course and the purpose to design such a course is analyzed. A survey is done by supplying questionnaires to the target

audience and a need assessment plan is constructed to identify the purpose of designing this course. Learner profile is made to identify learner characteristics in the analysis phase.

Design phase

At this phase a course map is designed in detail to show the flow of the course content.

Development phase

At this stage the course will be developed using Moodle. The activities will be developed using flash, online animation tools, Articulate, etc..

Implementation phase

During this stage the developed system will be hosted online. The Moodle LMS will be installed in the school and give the access to students to use it in the school as well as at home.

Evaluation phase

At each stage formative testing is done and summative test will be done for the content. Errors will be handled at this stage.

Chapter 3: Planning and Analysis

There are many ways of resolving the problem in the analysis stage, the most appropriate solution for the problem will be determined. In this Chapter the author has gathered the requirements from various ways resources using different requirement gathering methods.

Requirement analysis is in its definition means the understanding of the customer needs and expectations of the proposed system. The requirement analysis is done as one of the most important stages of the software development life cycle. Requirement analysis will try to find the need and the gap between the user expectation and developer's desired.

3.1 Stakeholders

Stakeholder Analysis is an important technique for stakeholder identification and analyzing their needs. First identify the important stakeholders who affect to the project and their interest. Following are the list of stakeholders directly affects the project.

3.2 Need Assessments

As the initial step of the analysis process a need assessment was conducted in order to identify the need for developing an online course for the Middle school children. A need assessment is the process of developing a blueprint for collecting needs assessments information.

3.2.1 The appropriate place to begin the Need Assessment

At the selected audience who's going to be trained by the awareness course and the authoritative who finds the need to start such a course. Hence would be the Asian International School.

3.3 Need Analysis

Before designing the course a need analysis should be conducted to assess what is the need of the key stakeholders to develop an e learning course as a solution.

1. Identifying the causes for the problem (objectives)

    i.   To find out whether the present education system in the school provide any opportunity for the children to learn about the Cyber safety issues in an online environment.

    ii.   To identify whether the present teaching materials include topics related to cyber safety such as, cyber bullying, pornography, sexting, grooming etc..

    iii.   To identify how taught content are delivered to the students.

    iv.   To identify the time barriers in the teaching process

    v.   To identify learner requirements such as the present knowledge of the learner about cyber safety, learning styles, learner capabilities, learner interests.

    vi.   To find out the activities involved in the classroom to teach these materials how they are being conducted at the moment. (student base, group activities, classroom games)

2. Target audience

Performers will be School children from 12 years to 16 years of age from the middle school.

    i.   **Decision Makers -** Principal, Deputy Principal, Sectional head of the middle school, authoritative bodies

    ii.   **Primary Users**- the students of the Middle School, who will be interacting directly with the Moodle Interface

    iii.   **Secondary Users**- the teachers teaching the students and parents of the students who are indirectly creates the opportunity to intervene with the course

      iv.   **Territory Users-** the authoritative parties, Principal, sectional heads

3. Methods of collecting data

      i.   Surveys- providing questionnaires to random samples from the selected samples

      ii.   Questionnaires [Appendix B]

          A questionnaire is a set of questions for obtaining statistically useful or personal information from individuals. It is rather practical and can be given to a large amount of people at once. However, It lacks validity, it has no way of telling how much thought a respondent has put in, also a respondent may be forgetful or not thinking within full context of the situation.

      iii.   Accessibility- the relevant focused groups can be physically contacted or individual interviews can be conducted. Surveys (questionnaires) are provided for children and parents.

4. Methods of Data analysis

A developmental data analysis would be done. The analyzed data will be presented using a spreadsheet model/graph.

5. How decisions will be made on the collected data

- The size of the population for the training
- The participant group
- The best method of communicating with participants or a sample of participants
- The multiple sources of data that might be helpful in understanding the need of the child learner

3.4 Learner Analysis

Learner analysis is the description of the target population. By analyzing the learner the characteristics that impact the learning and instruction can be rectified.

Few tools can be used to conduct the learner analysis;

- Surveys
- Observations
- Interviews
- Existing reports
- Test scores

For the proposed system the survey tool was selected to conduct the learner analysis as it is cost convenient and easy to conduct as the target audience is the school children where the author teaches.

Survey can be a very efficient method of gathering data with regard to the awareness of Cyber threats and security options. This can be done by way of questionnaires given out to students to fill and return. Participants can remain anonymous if they wish so. Data could be easily tabulated for reference. The disadvantage is that questions are pre-set, therefore cannot be modified or updated.

Having determined the need which should be addressed with the course, a questionnaire was prepared with related to Cyber Safety issues faced by middle school children.

The survey for the target audience was conducted for a selected sample under the guidance as the questionnaire contained few vague questions. Thus, false expectations were minimized through the results of the survey.

The learner analysis was done based on the Dick and Carey ISD model approach:

According to the model analyzing learner and context was one of the features of the instructional design model.

Intended and appropriate target audience- both males and females of the middle school section in the school between the ages of 11 to 15 years of age

demographics; identify characteristics directly related to the skill to be taught; and perform analysis of the performance and learning settings has to be analyzed of the learner of the target audience of this system.

3.4.1 Learner Related characteristics

Learners are not all like. Each learner of different backgrounds and individuals differ in the way they learn best. Instructions should be prepared keeping these considerations in mind. To make a successful instructional material the Instructional designers should consider the characteristics of the target audience.

It is assumed that learners are skilled with basic computer knowledge with how to view a video, how to use the internet, how to use Google search, read and understand a demonstration, etc.

Learns should be competent in English as all the materials are done in the English medium and have the ability to read and understand the instructions or guidelines.

Most of the learners are considered to be non major group of students of the relevant area who does not have prior experience and have no familiarity to use an e learning course. Further, the learners are also with different thinking and attitude patterns. Such as, some learners think it's not wrong to reveal personal information to a stranger, where as some other learners believe it is not safe. In addition the learners of this age group may not even realize that they could be addicted to digital devices and may not even realize the gravity of the negative psychological impact of it. Playing games with digital devices seems to be one of the most regular and favourite activity among them regardless of male or female.

 It was found out that the learners of the target audience was physically stable and in a good condition.

Fig -3 shows that most of the learners liked to play online games and are online savvy; therefore they prefer creative and interactive online material to learn with.

Target audience also consists of the decision makers. Therefore, a questionnaire was provided for the staff as well. According to fig-8 shows that 90% of the staff feels that an e learning solution would be interactive, instantaneous and collaborative.

3.5 Facilitator Analysis

The facilitator would be the author as the instructor of the Information Technology and two other teachers from the IT Department of the school. Teachers of the IT Department are subject experts and also possess considerable technical knowledge and skills to support the students.

3.6 Content Analysis

Content analysis is intended to, identify and isolate single idea or expertise units for instruction.

For the said course an original structured syllabus was not been able to identify. The referred similar resources were not applicable to the requirements of the target audience. Therefore, a new syllabus was constructed based on the existing syllabus provided by the CERT and the Ministry of Education, Malaysia (online) [Appendix B]

The content of the syllabus was designed based on the assumptions made by the analysis of data of the Questionnaire. .

Syllabus

LEARNING OUTCOMES

After successful completion of this course students will be able to:

- Define terminologies, concepts related to Cyber threats and dangers that children at Key Stage 1-3(Grade 7-9) face when engaged with ICT technology.
- Describe the ways that children would face threats and dangers in the online environment.
- Apply the e-safety methods and strategies to prevent risks and dangers hidden in the online environment
- Recall preventive strategies used with data security and personal safety when engaged in the digital world
- Analyze the different types of risks and problems related to digital media and how to mitigate them when using in their daily life
- Propose suggestions for any given situation with related to the use of online media.

- Revise the best practices of safety principles and strategies related to the cyber environment.

Topic	Hours
1- Need for Internet Safety and Information Security	04
2- online reputation and self expression- personal safety	04
3- Data security, laws and copyright infringements	04
4-Cyber world part-1-Apps, digital media and Addiction to digital media	05
5- About Cyber world part-2- balance online/offline	05
6- Online Bullying and negotiation/reconciliation	06
7- Dangers of Cyber Contacts	06
8- psychological impact in online usage and counselling	04
11- Final Assessment	**01**
Total for the course	**40**

Lesson 1- Dangers with Cyber Contacts (8 hours)

Instructional Objectives

- List different types of dangers with Cyber contacts
- Interpret your own ideas about cyber dating
- Apply the knowledge on dangers of sharing personal information in activities
- Construct solutions to given scenarios

    1. Dangers with Cyber Contacts

    1.1 Introductory video
    1.2 Activity- Discussion forum
    1.3 Lesson- Surprising dangers of sharing personal information online
    1.4 Lesson- Different ways your personal data can be shared online

Activity Quiz
1.5 Posting pictures- threats and preventions
1.6 Dangers in Cyber Dating and Cyber Pals
1.7 Cyber Crime
1.8 Cyber pornography and sexual Interaction
1.9 Prevention methods of Cyber dangers

Unite 1 Assessment

Lesson 2 – Online Reputation (6 hours)

Instructional Objectives

- Define Online Reputation.
- Learn the importance of having a positive online reputation.
- Learn the consequences of a negative online reputation.
- Use sound judgments before posting or commenting on social media.
- Collaborate with peers and identify the responsibilities in using the online in a positive way.

2. Online posting and online reputation
   2.1 What is Online Reputation?
   2.2 Reputation in school life and online
   2.3 How does sharing posts affect Online Reputation?
   Activity- Jigsaw puzzle
   2.3 What is Digital Footprint?
   Activity- Create their own footprint and share
   2.4 What could affect your Online Reputation?
   2.5 Tips for a positive online reputation
        2.5.1 Poster- Tips to make a positive online reputation

Unit Assessment 2

Lesson 3- Cyber bullying (6 hours)

Instructional Objectives

- Define what is online bullying
- Learn the consequences of Cyber bullying
- Practice tips to prevent cyber bullying

- Revise the knowledge on cyber bullying

    3.1 Introduction to online bullying

    3.2 Causes behind Online Bullying

    3.3 Negative consequences of Online Bullying

        Activity

    3.4 Tips and checklists to prevent cyber bullying

    3.5 Importance of practicing Netiquette

    Unit Assessment 3

Lesson 4- Digital Addiction (8 hours)

Instructional Objectives
- List different types of addiction to Digital Media
- Recall the symptoms of online addiction
- Watch a movie and interpret your ideas on digital addiction
- Categorize different types of digital addiction
- Construct your own ideas of digital addiction in activities

    4.1 Introduction on addiction to Digital Media

    4.2 Different types of addiction and its effects on us

        Activity

    4.3 Effects of addiction on Social Media, Smart phones and Online Games

        Activity

    4.4 Best practices to prevent addiction

        Unit Assessment 4

Lesson 5- Psychological impact of digital use (4 Hours)

Instructional Objectives

- list the ways you can be psychologically affected by using online

- practice recalling the features of psychological impact

- construct solutions to given scenarios about psychological defects due to use of excessive online

5.1 Introduction to Internet use and it's psychological effect

5.2   Different ways you can be psychologically affected by over using online
         Test yourself- Has the web affected you?

5.3   Top psychological effects of Internet on humans

5.4   Personality disorders caused by the Internet

Unit Assessment 5

Lesson 6- Internet Safety and Reporting Crime (8 hours)

Instructional objectives

- define how to safely search the Internet
- apply their knowledge on how to prevent from fake profiles and safeguard their personal details
- analyze the unsafely areas in the Internet and suggest solutions to prevent them

  6.1 Introduction to Safe searching on the net

  6.2 safe searching tips -how smart are you when searching information online

  Activity

6.3 Preventing from fake profiles and hacking

6.4 Who are online scams and pedophiles on the Internet?

6.5 Smart tips to avoid unsafe contacts online

Quiz Activity

6.6 Tips for Cyber Wellness

6.7 Reporting crime

Unit Assessment 6

3.7 Descriptive Analysis of the collected data

This study was conducted with the aim of identifying the risks and threats related to online savvy among the children of the age group from 12 to 15 years of the Asian International School.

In order to achieve the above objective, a sample of 50 students was selected from a 150 student group of the middle school of the Asian International School, Colombo. The sample was selected based on a sampling frame, which is the register of each class where all the names of the students are recorded in the register. 50 random numbers were taken from a random number table, to select a sample of 50 students.

The following data were collected:

- Mode of accessing Internet- Parent's guardian's computer at home, Own computer at home, Own laptop, Mobile phone, Internet café, Friends House, School, Other

- Whether they play online games: yes,no

- The device used to play games- xbox, play station, pc, laptop, tablet, Nintendo wii, other
- Awareness about privacy and security settings: yes/no
- Hours spent on the Internet during weekdays: 0,1,2,3,4,5 or more
- Hours spent on the Internet during weekends: 0,1,2,3,4,5 or more

- Frequency of communication about internet with parents/ guardians: never, rarely, sometimes, regularly

- Extent of rules imposed by parents regarding Internet use: no rules, access restrictions, time restrictions, access and time restrictions
- social network sites visited: Facebook, Twitter, Instagram, Snapchat YouTube, Skype, Facetime, Other

- the biggest threat faced online: Bullying or harassments by friends or acquaintances, unwanted sexual approaches in a chat room, social networking site, email, coming across sexual images, content, someone is using my photo in an inappropriate way, someone taking my photo and circulating them, None of these, other ways

- Awareness about blocking and reporting on social networks Yes, No

- Awareness on whom to inform about cyber threats faced online: Yes, No

- Number of times (0,1,2-5,more than 5) they are exposed to the following situations online: Added a stranger to the instant messenger contact list, Add a stranger to a social networking friend list, spoken on the phone to someone you met online revealed your true personal details online.

3.7.1 Summary of Data

Following are the summarized details which were taken from the given questionnaires.

The total number of students in the total three grades is about 150. The sampling method was conducted based on the sampling frame where number of students is recorded by their registration number. The entire set of data was taken as a whole and from a random table 50 random numbers were selected.

Out of the 50 students, 28 were males and 22 were female students. 25% of the students are Sinhalese and Christians and 10% of Muslims and 10% of Hindus and 5% of foreign students (Korea, India and Maldives). All the students are representing the age category from 12 years to 15 years of age. 1 or 2 Sri Lankan students were with Canadian citizenship.

3.7.2 Conclusion

According to the Table summary

1. In the sample, a vast majority of 58% of the students are accessing the internet by the use of a mobile phone. (Refer Appendix A – Table 01)

2. It is found out that more than 80% of students play online games. (Refer Appendix A – Table 12)

3. Out of the 50 students, most play games using their laptop or tablet which are 62% and 60% respectively. Only about 18% of the students use Xbox to play games and Nintendo wii is used by 20% of the students. (Refer Appendix A – Table 03)

   - There is an increasing trend to use Nintendo and x box which poses a major influence towards game addiction

4. A significant percentage of students about 36% are not aware of privacy settings (Refer Appendix A – Table 04)

5. Only 36% of the students communicate regularly with parents. So the remaining 64% of the students do not engage in frequent communication with their parents. (Refer Appendix A – Table 05)

   - Without frequent communication with a responsible adult they are highly vulnerable to cyber threats. It is less likely to talk with parents about their personal use therefore counseling is needed

6. 34% of the students have no restrictions imposed on their internet use by parents. Only 12% have access restrictions. A very low percentage of 2% only has both time and access restrictions imposed on their internet use. (Refer Appendix A – Table 06)

   - if there are no time limits they can get addicted to internet easily

7. Youtube and Instagram are the most visited social network sites, 76% and 50% respectively. Every social network is used by approximately a quarter or more of the students in the sample. 92% of the students visit at least one social network site. (Refer Appendix A – Table 04)

   - It has become a norm therefore, every child will be exposed to the features of it

8. 32% of the students experience bullying or harassments as the biggest threat online, while 28% of the students think coming across sexual content is the biggest threat online. Unwanted sexual approaches are regarded as the biggest threat by 26% of the students. (Refer Appendix A – Table 05)

9. 44% of the students spend 4 or more hours on the Internet on weekdays (Refer Appendix A – Table 01)

10. Students spending 4 or more hours during weekdays suggests that students are unnecessarily spending more time online at the expense of studies and outdoor games and human interactions, in turn it would decrease health condition (Refer Appendix A – Table 03)

11. About half of the students spend more than 5 hours on the Internet during the weekends.
    - Main mode of leisure activities has become the use of online thus need to balance online and offline

12. 60% of students do not have the knowledge on how to use the block options. (Refer Appendix A – Table 11)

13. 65% of students recorded that they do not have knowledge on how to get advice from an adult at the time of online harassment.
    - They need to be knowledge about report and advice

14. 74% of students have added a stranger to their contact list at least once. 64% of the students have spoken at least once on the phone to someone met online. 76% of students have revealed their true online at least once (Refer Appendix A – Table 08)
    - Thus, the students needed to be educated the fallacy behind creating relationships with strangers and revealing the true details in the online setting

15. 65% of students do not add a stranger to a social networking at all, whereas 12% of them have added at once and two to five times, while 8% of students have added more than five times.

- According to this there is a low trend in adding strangers' contacts in the social networks, whereas through their instant messenger there is a high trend of adding strangers. This seems to reflect an ambiguity in the question since the exact name of the social networking sites have not been specified, therefore the analysis was done excluding this question.

As there was no standardized format of the syllabus for the Cyber safety Issues found in Sri Lanka or foreign context, the proposed syllabus was designed based on the module outline of CERT(**Computer Emergency Readiness Team | Co-ordination Center** of Sri Lanka), the subject expert of this area of studies and a complied syllabus on Cyber Safety Issues of Education Ministry in Malaysia. [Appendix D]

After analyzing the data gathered from the questionnaire, it was found out that some of the topics of the above syllabus are irrelevant for the requirement needed. However, some of the topics of the syllabus of the CERT were included under the guidance of the subject expert.

3.7 Newly designed syllabus for the Cyber Safety course

As a formal properly structured syllabus did not exist for the proposed course, it was a challenging task for the author. However, a new syllabus was structured based on few existing syllabuses online. The syllabus compromises, need for Internet Safety, online reputation, data security laws, addiction to digital media, balancing online usage, online bullying, dangers of Cyber contacts, psychological impact of over use of the Internet, whom to report and seek advice.

The duration for the syllabus will be approximately 50 hours. Assessments and activities will be designed based on the learner capacities. (Refer Appendix A)

3.8 Analysis of Learner Achievements

Learners will be assessed through interactive game based learning environment. The Cyber Safety course is intended to create awareness and attitude change of the learner. All the assessments are based on the learning outcomes and are not set as exam type tests. As the learner is focused towards an emotional, psychological change in the mind set experientially they will acquire the knowledge through the quizzes which are enjoyable. At the end of the sub unit activities, learners can earn rewards such as badges or starts to increase their total score high.

3.8 Context Analysis

This is a method to analyze the internal environment of the organization. The purpose of this study is to ensure that that the project is informed by all of the contextual factors that might affect the implementation and the sustainability. For the proposed system it is important to do a context analysis as it will feature out who you are, your network of contacts, your experience and what your organization can do in terms of internal resources and capabilities.

The context analysis will be done by identifying what to be achieved from the project, focusing on the specific area to be analyzed and the analysis.

The students of the Asian International School are a hub for discovering new technology and expanding knowledge through the use of the Internet. According to the survey findings [1] 90% of students access the Internet through their smart phones or Tablet devices. The school too exposes children to many avenues of academic streams through Internet for a better performance of grades. More, specifically technology brings many benefits for middle school students, as the abstract concepts of subjects can be visualize for a better understanding and students are more likely to understand topics through a web based inquiry unit which includes visualization.

However, the children of the middle school are of ages from 11 to 15 years. Since they are at a very sensitive age, the risks that could affect them are crucial. They could be easily affected negatively by the Internet. According to the researches most of the European schools have introduced many safety actions and precautions as a remedy for the threats and risks of the online usage. However, Sri Lanka is still lagging behind in taking constructive actions.

According to the wordings of a resource person of the National child protection authority, still the awareness courses about cyber threats are at the early stages.

However, the authoritative of the Asian International School Colombo, has rectified the urgency of such an awareness course for the students due to a consecutive number of incidents occurred among the children of the school.

A quite reasonable amount of evidences were identified in order to propose the need for an awareness course;

According to the finding done at the survey [2], the use of social networking in the middle school is at a considerable high rate. WhatsApp, snap chat, twitter, Facebook are used to mostly chat with friends or strangers. These activities may expose the students share personal information without proper knowledge. As a result, Internet offenders and predators could cause harm for the children.

Majority of students stated that they use their smart phones or other digital devices for online games and some of them are severely addicted to playing online games and social networks. As a result, there seems to be a progress in the ill-behaviour among the students. Many of the students are being given cautionary warnings and suspensions due to lack of concentration, indecent acts in the class and hyperactive behaviours, which is suspected due to the addiction to online games which activates hyper psyche and violence.

Further, Cyber bullying has become another main issue in the school which has resultant to keep a halt mark in their school carrier. As much as technology is beneficial to the students through creating and sharing knowledge with each other, there are possibilities that some students may exploit it and cause harm to others.

Moreover, illegal use of the Internet would also be a critical threat to the middle school students. Illegal materials can vary from prohibited distributions to copyrighted materials, where the students are not known about.

Dr.B.J.C Perera MBBS (Ceylon), DCH (Ceylon), DCH (England), MD (Paediatrics), FRCP (Edinburgh), FRCP (London), FRCPCH (United Kingdom), FSLCPaed, FCCP, FCGP (Sri Lanka), Consultant Paediatrician in one of his report stated that Cyber Bullying is most common in the middle school ages and he further mentioned, *"Schools can be very effective brokers in working with the parents to stop and remedy cyber bullying situations. They can*

also educate the students on cyber-ethics and the law. If schools are creative, they can sometimes avoid the claim that their actions exceeded their legal authority for off-campus cyber bullying actions. We recommend that a provision is added to the school's acceptable use policy reserving the right to discipline the student for actions taken off-campus if they are intended to have an effect on a student or they adversely affect the safety and well-being of student while in school. "

In accordance with the above statement, it could be learnt that an E learning course would be an ideal instructional solution to teach about being safe from online threats and teach students how to be a healthy digital citizen. As the existing system does not provide any mode of classroom teaching with related to the awareness of cyber threats and only annual workshops are conducted which are not cost effective.

Further, there are students with different standards of knowledge with different expertise, thus a classroom teaching cannot cater all at once but an interactive online course could provide the opportunity for different level of knowledge simultaneously. Therefore, the proposed online course could effectively engage the all the students in the awareness course.

Considering all the above reasons, I believe that teaching awareness on cyber threats to middle school students is very important. If the students were properly educated about the online threats, digital laws the unnecessary problems could be mitigated.

3.9 Readiness for e learning Analysis

3.9.1 Financial readiness

The institute's mission is to facilitate the learners with latest technologies and methods and therefore e learning is an ideal solution. The management and the parents' committee of the school are ready to invest initial fund programs for the e learning course.

3.9.2 Infrastructure readiness

The school is possessed with three labs equipped with necessary hardware and software and a well maintained server. Internet connections to the machines are provided throughout. Therefore, the course can be used by the learners at any time that will be planned.

3.9.3 Cultural readiness

The Staff of the computer department was unfamiliar to the e learning installation except for the author. Therefore a small training with an introduction session was conducted for the staff to show the importance of an e learning course.

Students were given an orientation of the programme and were taken back their feedback of the response towards the programme. The students of the middle school are skilled in the use of IT technologies and most of them are visual learners. They prefer active learning with different types of interactions. All of them are not disabled but there are few slow learners.

3.10 SWOT Analysis

Strength-Weaknesses-Opportunities-Threats Analysis (SWOT Analysis) is a tool for investigation and decision making. SWOT analysis is used for a variety of purposes in business and by different kinds of organizations - including schools. SWOT analysis promotes brainstorming.

The SWOT Analysis of the Asian International School for the implementation of a Cyber Safety course for the Middle School children is as follows:

Strengths	Weakness
- Most of the users are having a good knowledge about ICT - The course contents can be reused by the students - Administration is funding for the hosting charges, etc - Learners are duly motivated to learn the e learning course	- Resistance of the staff to get used to the system - Maintenance of the hardware system is poor - Some of the students are slow learners who need extra timings and help.

Opportunities	Threats
• Deviation from a traditional classroom to a fulfill environment • Opportunities to get familiarize to latest technologies	Students can be adopted to depend on totally e learning subjects

Table 3.1 SWOT Analysis

3.11 Task Analysis

A Task Analysis consists of a written list of the discrete steps required to complete a task. The Task Analysis is never given to the child but is used by the teacher and staff supporting the student in learning the task in questions.

A Task Analysis for designing the project:

1. Select syllabus from online sources about Cyber Safety Issues
2. Select online courses developed on this topic to identify the syllabus structure
3. Carefully read and understand the relevant areas needed for the proposed system
4. Select areas needed to design MCQ questions
5. Make quizzes and answers for each question bank
6. Make videos and animations interactively using open source tools
7. Import youtube videos
8. Develop videos using Adobe premier to make the lessons interactive
9. Create interactive activities such as, puzzles, games, presentations, paint tool etc.
10. Create student login
11. Students of the Middle School follow the course in the school for two hours each week
12. Students take up the course for 8 months
13. Other students can use it from home by getting access to the system
14. Students play a game and learn the content
15. Students watch a movie and learn the content
16. Students receive reward badges in completion of quizzes
17. Close the system.

Chapter 4: Design

Similar to the planning and analysis chapter, this chapter discusses about the methodology and tools adopted for the purpose of designing the prototype to achieve a better understanding of the proposed system.

The design methodology can be used to model each highlighted element into a diagram that can be used to clarify implementation design.

4.1 Methodology

Author used the ADDIE as the ISD model to design the course on Cyber Safety as defined in the Chapter 2.

As a proper structured syllabus was not identified compatible to the requirements or needs, a newly structured syllabus was designed under the guidance of the subject expert at CERT and the head of the Middle school section of the Asian International school and referring the online sites [Ref: Appendix A] from the scratch. A copy of the certification approval for the designed syllabus by the head of the Middle School section is attached. (Refer Appendix B)

4.2 Design Considerations
When designing the course following were considered.

Time
The course should be developed within six months. All the phases: analysis, design, development, implementation and evaluation should be done within this time period.

Authoring software
Selection of the software to develop the course is an important task. Since there are several authoring tools to develop an eLearning course, alternatives should be tried and the best tools should be selected.

Required resources
Since the developer is new to the subject child psychology, thorough literature review was done. In addition views of subject matter experts and the college principal also considered.

Course Accessibility

Since the learners are having internet connections with different bandwidths, course will contain image, audio and video files with small file sizes. It will help learners with low bandwidth internet connection to access the course without difficulty.

Design of Course content

Organization

Content and activities were arranged sequentially. They are interactive and help to engage the learners in activities. Information were "chunked" and arranged sequentially from simple to complex.

Navigation

Appropriate navigation were designed, with Next and Previous buttons.

Assessment

Interactive assessments such as Drag and drop questions and MCQs with constructive feedback will be given to the learners.

Design consideration.

Gagne's 9 steps of an instruction

9 steps of multimedia instruction

Interactivity design

Quiz design

Assessment design

4.3 Syllabus

LEARNING OUTCOMES

After successful completion of this course students will be able to:

- Define terminologies, concepts related to Cyber threats and dangers that children at Key Stage 1-3(Grade 7-9) face when engaged with ICT technology.
- Describe the ways that children would face threats and dangers in the online environment.

- Apply the e-safety methods and strategies to prevent risks and dangers hidden in the online environment
- Recall preventive strategies used with data security and personal safety when engaged in the digital world
- Analyze the different types of risks and problems related to digital media and how to mitigate them when using in their daily life
- Propose suggestions for any given situation with related to the use of online media.
- Revise the best practices of safety principles and strategies related to the cyber environment.

Topic	Hours
1- Need for Internet Safety and Information Security	04
2- online reputation and self expression- personal safety	04
3- Data security, laws and copyright infringements	04
4-Cyber world part-1-Apps, digital media and Addiction to digital media	05
5- About Cyber world part-2- balance online/offline	05
6- Online Bullying and negotiation/reconciliation	06
7- Dangers of Cyber Contacts	06
8- psychological impact in online usage and counselling	04
11- Final Assessment	**01**
Total for the course	**40**

Table 4.1 Syllabus

4.3.1 Synopsis/overview

This course introduces the threats and risks of online savvy and creates awareness among the students on strategies and protection methods when using Internet. This course will make the students aware on the areas which are negligible to students in an online environment.

4.3.2 PEDAGOGICAL FRAMEWORK

The main pedagogical framework of the course focuses on activity based interactive learning. Students are supposed to do all the learning activities to cover the learning content. As this course is designed for children between the ages of 11 to 15 years, the syllabus was chunked to sub units and each unit consists of an interactive activity. The lesson starts with an ice breaker such as an interactive movie or discussion forum. Each lesson consists of practical activities using software which they are familiar to learn the lesson. Therefore, by doing these activities eventually they will gain the knowledge about cyber threats.

4.3.3 EXPECTATIONS/EXAMINATIONS/REQUIREMENTS

At the end of each lesson a quiz activity will be given to check the knowledge before going to the next module and each of these assignments are not created in an exam oriented setting as this is focused to give awareness in an enjoyable way. The learners are expected to obtain knowledge on the key areas of e-safety and its adverse effects. There will be series of continuous assessments on each module covered and an overall quiz at the end of the course at the end of the full syllabus.

4.3.4 DETAIL SYLLABUS

Lesson 1- Dangers with Cyber Contacts (8 hours)

Instructional Objectives

- List different types of dangers with Cyber contacts
- Interpret your own ideas about cyber dating
- Apply the knowledge on dangers of sharing personal information in activities
- Construct solutions to given scenarios

    1. Dangers with Cyber Contacts

1.10   Introductory video
1.11   Activity- Discussion forum
1.12   Lesson- Surprising dangers of sharing personal information
        online
1.13   Lesson- Different ways your personal data can be shared online
        Activity Quiz
1.14   Posting pictures- threats and preventions
1.15   Dangers in Cyber Dating and Cyber Pals
1.16   Cyber Crime
1.17   Cyber pornography and sexual Interaction
1.18   Prevention methods of Cyber dangers

Unite 1 Assessment

Lesson 2 – Online Reputation (6 hours)

Instructional Objectives

- Define Online Reputation.
- Learn the importance of having a positive online reputation.
- Learn the consequences of a negative online reputation.
- Use sound judgments before posting or commenting on social media.
- Collaborate with peers and identify the responsibilities in using the online in a positive way.

2. Online posting and online reputation
    2.1 What is Online Reputation?
    2.2 Reputation in school life and online
    2.3 How does sharing posts affect Online Reputation?
    Activity- Jigsaw puzzle
    2.3 What is Digital Footprint?
    Activity- Create their own footprint and share
    2.4 What could affect your Online Reputation?
    2.5 Tips for a positive online reputation
            2.5.1 Poster- Tips to make a positive online reputation

Unit Assessment 2

Lesson 3- Cyber bullying (6 hours)

Instructional Objectives

- Define what is online bullying
- Learn the consequences of Cyber bullying
- Practice tips to prevent cyber bullying
- Revise the knowledge on cyber bullying

3.6 Introduction to online bullying

3.7 Causes behind Online Bullying

3.8 Negative consequences of Online Bullying

Activity

3.9 Tips and checklists to prevent cyber bullying

3.10   Importance of practicing Netiquette

Unit Assessment 3

Lesson 4- Digital Addiction (8 hours)

Instructional Objectives
- List different types of addiction to Digital Media
- Recall the symptoms of online addiction
- Watch a movie and interpret your ideas on digital addiction
- Categorize different types of digital addiction
- Construct your own ideas of digital addiction in activities

4.1 Introduction on addiction to Digital Media

4.2 Different types of addiction and its effects on us

Activity

4.3 Effects of addiction on Social Media, Smart phones and Online Games

Activity

4.4 Best practices to prevent addiction

Unit Assessment 4

Lesson 5- Psychological impact of digital use (4 Hours)

Instructional Objectives

- list the ways you can be psychologically affected by using online

- practice recalling the features of psychological impact

- construct solutions to given scenarios about psychological defects due to use of excessive online

    5.5 Introduction to Internet use and it's psychological effect
    5.6   Different ways you can be psychologically affected by over using online
        Test yourself- Has the web affected you?
    5.7   Top psychological effects of Internet on humans
    5.8   Personality disorders caused by the Internet

    Unit Assessment 5

Lesson 6- Internet Safety and Reporting Crime (8 hours)

Instructional objectives

- define how to safely search the Internet
- apply their knowledge on how to prevent from fake profiles and safeguard their personal details
- analyze the unsafely areas in the Internet and suggest solutions to prevent them
                6.8 Introduction to Safe searching on the net
                6.9 safe searching tips -how smart are you when searching information online

                    Activity

    6.10   Preventing from fake profiles and hacking
    6.11   Who are online scams and pedophiles on the Internet?
    6.12   Smart tips to avoid unsafe contacts online
    Quiz Activity

    6.13   Tips for Cyber Wellness
    6.14   Reporting crime
        Unit Assessment 6

4.4 Course Map Level 1

Course Map Level 1 of the design level briefly describes what are the levels and sub levels of the actual course content by showing paths to develop the functionalities and course contents of the system.
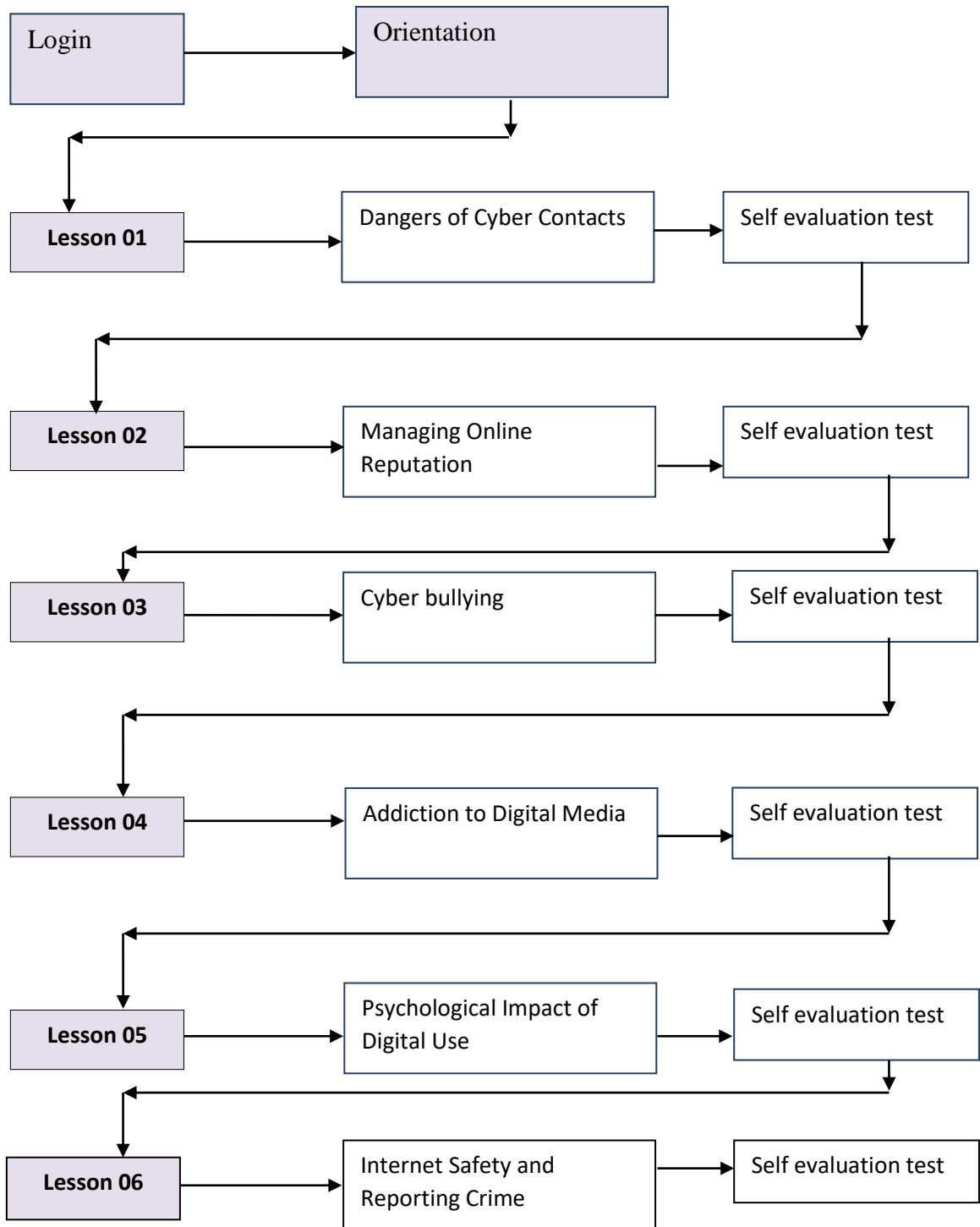
4.2 Top Level Course Map

4.5 Detail Course Map

Course Map Level 2 is derived from Course Map Level 1, and it shows a rough sketch of detailed paths of the flow of the system.
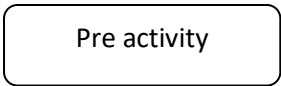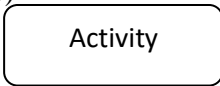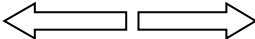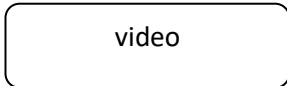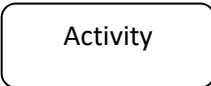
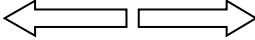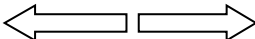**Lesson 1- Dangers of Cyber Contacts**
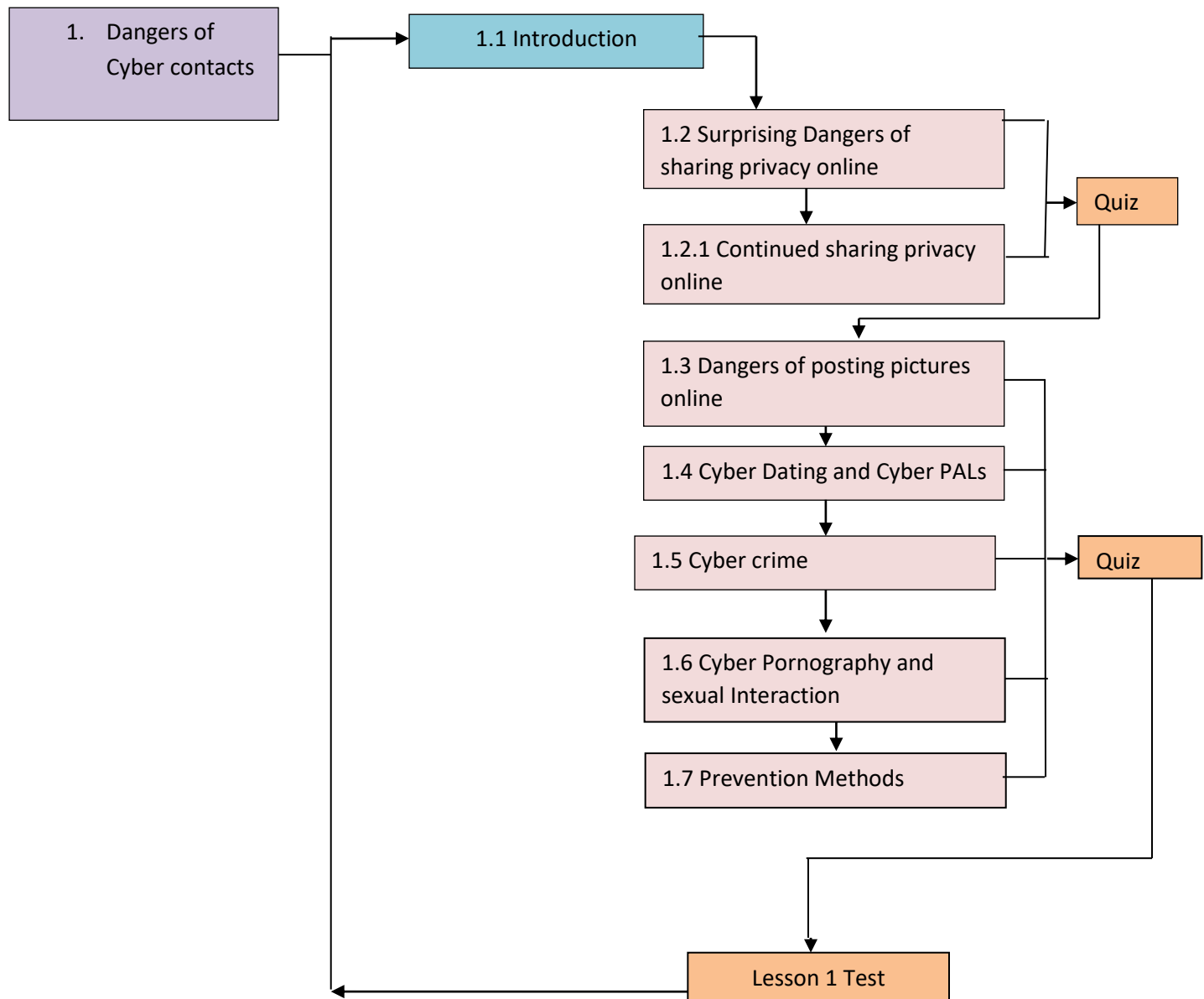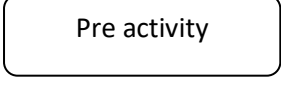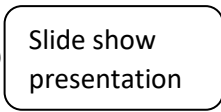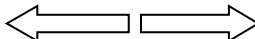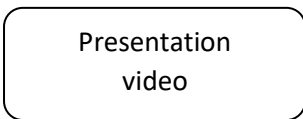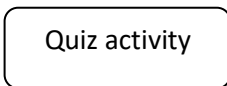
Figure 4.3 Detail Course Map of Lesson 1

4.6 Top Level Storyboard

Storyboards are the blueprints of an interactive courseware design and development process. They provide a combination of text and graphics or graphic descriptions that convey all the necessary information about the delivery of course content. Storyboards describe in detail all images, animations, movie segments, sound, text and navigational paths.

Module 1- Surprising Dangers of Cyber Safety

Visual	Explanation
a) Pre activity b) Activity	a) Ice breaker– watch a movie about dangers of sharing information online. b)present their thoughts about the movie with peers using a discussion forum
a) Pre activity b) Slide show presentation	a) pre activity- drag and drop game to familiarize the Cyber Threats b)presentation on sharing personal privacy
a) Presentation video b) Quiz activity	a) video about posting pictures online threats and preventions b)Activity quiz-MCQ on sharing personal privacy online
a) video b) Activity	a)video presents cyber crime b)assessment activity- interactive video is used to check the knowledge

	a) Pre-activity- sharing opinion about cyber dating using forum
a) Pre-Activity b) Presentation video c) Activity ⇐ ⇒	a) Pre-activity- sharing opinion about cyber dating using forum b) Presentation video on cyber dating c) Drag and drop activity on what the students learnt about cyber dating
a) Text resources b) Activity ⇐ ⇒	a) Text resources on preventing cyber crimes b) Answer MCQ questions

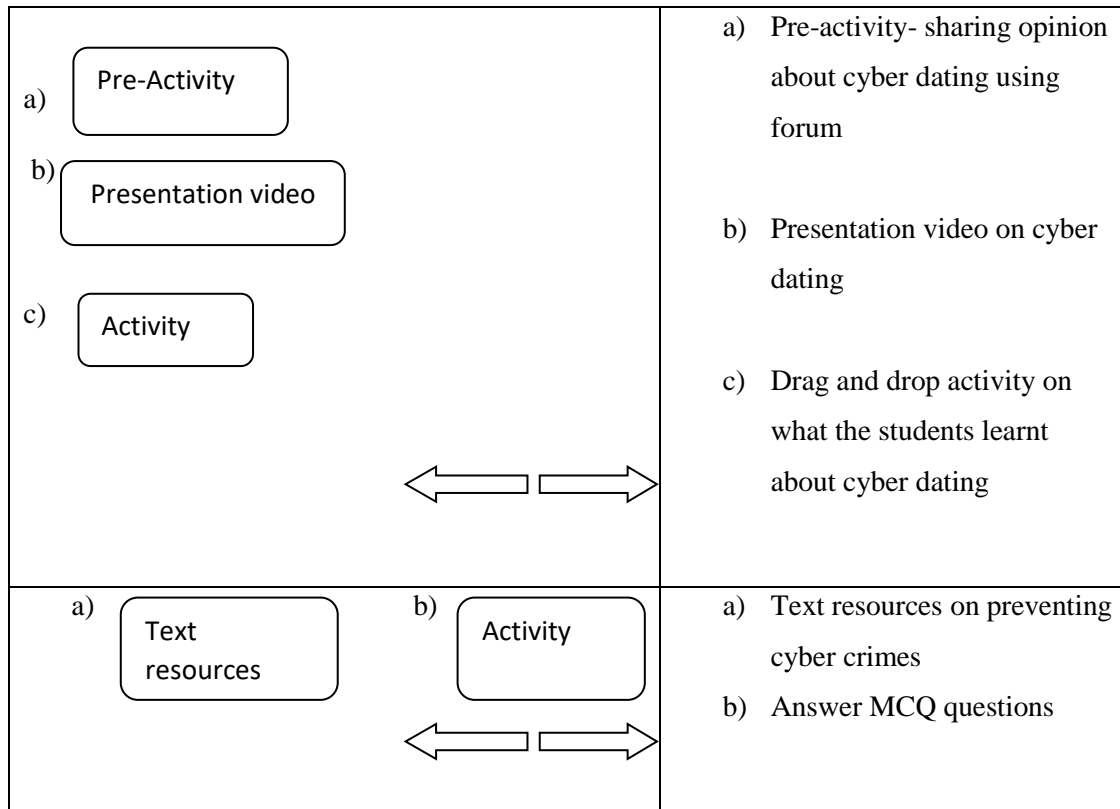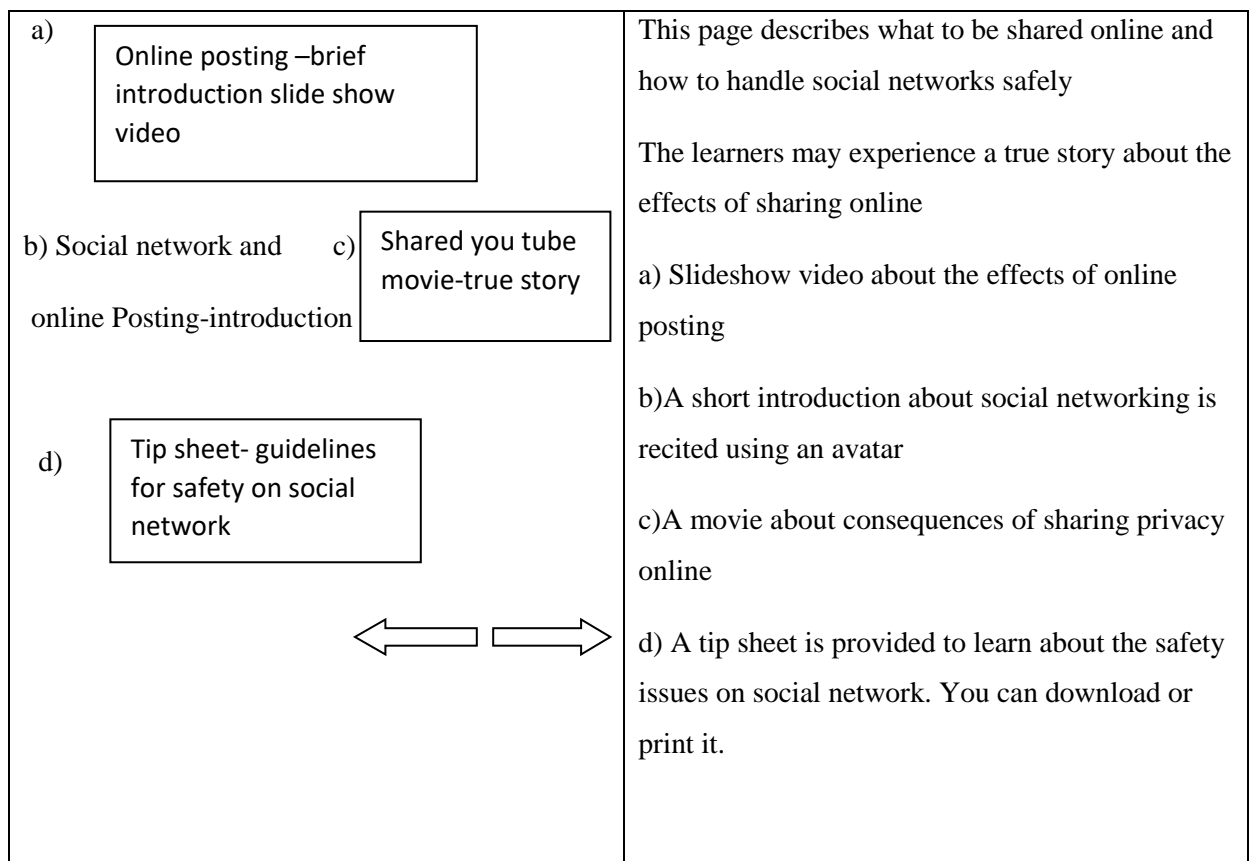*Figure 4.3 Top Level Storyboard Lesson 1*

Module-2 online reputation

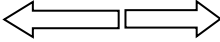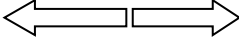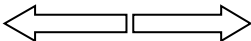|	This page describes what to be shared online and how to handle social networks safely
a) Online posting –brief introduction slide show video b) Social network and online Posting-introduction c) Shared you tube movie-true story d) Tip sheet- guidelines for safety on social network ⇐ ⇒	This page describes what to be shared online and how to handle social networks safely The learners may experience a true story about the effects of sharing online a) Slideshow video about the effects of online posting b)A short introduction about social networking is recited using an avatar c)A movie about consequences of sharing privacy online d) A tip sheet is provided to learn about the safety issues on social network. You can download or print it.

Quiz Activity ⟵⟶	. Their analytical skills are checked with this activity The learners will read a small case study and prepare a chart including the problems, threats and solutions/precautions that come across in the scenario. Pictures are provided in a separate folder. Submit to the assignment link.
How can it harm you- visual aids Text description- digital footprint and digital shadow ⟵⟶	This page will give a visual display on how digital footprint can harm your life. Text introduction is given about digital footprint. visual aids are provided on this topic
Quiz- Game-Interactive ⟵⟶	Testing the knowledge on digital footprint

Figure 4.4 Top Level Story Board Lesson 2

Module -3 Cyber Bullying

a) Slideshow video b) YouTube movie c) Quiz Activity ⟵⟶	a)slideshow presentation will present about what is online bullying and facts of bullying b) movie- students will learn the consequences of bullying c) The students will create their own story on cyber bullying using Desktop Publishing or Ms Paint.

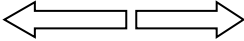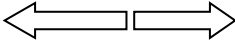|	
a) Pre activity b) Cyber bullying prevention Tips c) Lesson explanation using Avatar ⟸⟹	This page describes about how to prevent cyber bullying a) Checklist form about prevention methods of Cyber Bullying is given for the students. Students will get the immediate feedback. b)Tips to prevent cyber bullying is presented in bullet points c) Using an avatar the students will be given an audio presentation with the visual images about developing values to prevent cyber bullying. Students learn Netiquette.
Assessment Activity ⟸⟹	Using wiki students will present their ideas about cyber bullying. They will use the guidelines of netiquette they learnt.

Figure 4.4 Top Level Story Board Lesson 3

Module 4 Addiction to Digital Media

a) [Pre activity] b [Slideshow video] c) [Poster and tips sheet] d [Activity] <⟺>	This page describes addiction to digital media and apps A) Pre-activity- Internet addiction quiz to get a familiarity on what is addiction. The students will get an immediate feedback. Based on the pre activity they will use the chat room to chat with peers to share their ideas about addiction. b)The slideshow video will explain about addiction to digital media and apps and consequences of it c) About dangerous apps that can be harmful. Students can download and print it. d) guessing game
a) [YouTube video] b) [Audio activity] c) [Slideshow presentation] <⟺>	This page describes about addiction to social media a)students can watch a movie about addiction to social media b) Short video clips are displayed where students can watch. c) Slideshow presentation will display about prevention tips for addiction. Students will be able to download/print a prevention tips sheet for their own use at the end of the video.
[Assessment Activity] <⟺>	MCQ quiz on addiction to digital media, social media its effects and prevention methods

Figure 4.5 Top Level Story Board Lesson 4

Module 5 Psychological Impact of Digital Use
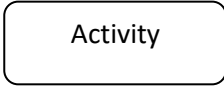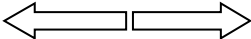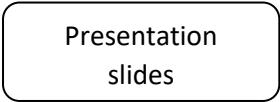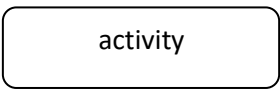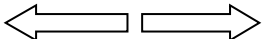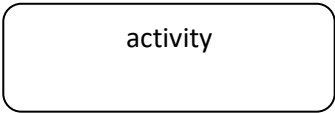
Visual	Explanation
a) Introduction [Image] b) [Image] c) [Activity] ⟸⟹	a)animated image with the introduction in text about the psychological impact of Internet b)The image of a brain is displayed interactively for the learner to click and learn different types of ways that can impact psychologically due to overuse of online c)Test yourself assessment quiz – a self check
a) [Presentation slides] b) [activity] ⟸⟹	a) presentation on top psychological effects of internet on humans and online gaming b)Assessment Activity- using a crossword puzzle students have to guess the correct name for the psychological symptom learnt
[activity]	Final assessment

Figure 4.6 Top Level Story Board Lesson 5

Module 6 Internet Safety and Reporting Crime
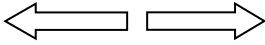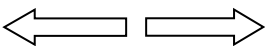
Visual	Explanation
Lesson 6- Internet Safety and Reporting crime a) Interactive presentation • Need for Internet Safety • Types of dangers in the cyberspace b)Activity- create their own presentation in power point as a summary on what they learnt and post it to the forum to share with peers c) Use visual aids to interactively teach best practices for Internet safety d) Activity-drag and drop about Internet Safety rules(fill in the blanks)	This page describes the need for Internet Safety and dangers related to the cyber use and how can you overcome the threats a) This presentation has interactive content(audio and video) b) Activity- creating their own presentation c) An interactive visual aids where the learner can click that and view an image of the content. Audio is provided to present the information related to it.
Lesson Quiz A matching activity to appropriately match the meaning to the correct word	Checks whether learners can understand the learner and can map the concepts with the real life situations

Figure 4.7 Top Level Story Board Lesson 6

4.7 Detail Level Storyboard

Storyboard- Module 1

Course Name: Cyber Safety Issues	Storyboard File no. 04.00
Course section: Module 1- Ice breaker	
Lesson Name: Dangers with Cyber Contacts	ID's name: NAW
Objective(s): • watch the dangers and threats in sharing personal privacy online • Interpret the personal views about sharing personal privacy • Play a game and familiarize the threats related to sharing personal information online	SME's name: NAW

Page Title: Title page –Dangers of sharing personal information online(ice breaker)	Page no. 00.04.01.00	CD's name:

7.

8.
Pretty easy to get your details!!

9.

10.
Would you ever reveal your true home Address to a stranger online?

11.
GUESS WHO?

12.
Put down your own thoughts about the movie
Click here

Special Comment(s): . Editing is done based on the following you tube video:

The play, replay, stop and pause buttons should be available in the video screen

1) (Starting background music-Ref-Audio Track 01) A girl of about 10 years with black hair and brown skin chatting in a desktop or smart phone, the room surrounding should be similar to Sri Lankan context.

(chat conversation is given in the audio as well, a voice of a small girl and a small boy)

2) The computer screen will be focused while the girl is typing, the screen should be zoomed to see the chat window with a blur effect on the screen.

(background music is provided-Ref-Audio track 01)

4) This text will appear in a different screen with a plain light blue background. The text should be bold and font colour is Dark blue contrasting the background colour and the text should be centred on the screen with a larger font size. (background music is provided)

6) This text will appear in a different screen with a plain light blue background before the chat partner is shown. The text should be bold and font colour is Dark blue contrasting the background colour and the text should be centred on the screen with a larger font size. (background music is provided)

Figure 4.8 Detail Level Story Board Lesson 1

Storyboard-Pre Activity-Discussion Forum

Page Title: pre activity- surprising ways of sharing personal information online		Page no. 00.04.02.00	CD's name:
Date Designed:	Date SME contributed:		Date verified:
Design			

Figure 4.9 Detail Level Story Board Discussion Forum Lesson 1

Storyboard-Pre-Activity

Page Title: **ACTIVITY: Pre-Activity – Danger and ways of sharing personal information online**	Page no. 00.04.03.00	SME's name:
Date Designed:08-08-2016		Date verified:

Design

Cyber Safety

Surf   Safely   Online

What is safe to share? Try out this Game and find out…..

Match the correct cyber threat with the given pictures. Drag and drop the textbox to the matching picture. You are given two chances each.

So glad to be home!

Scam

(Good Attempt! Try Again!)

(Awesome guess!!)

Fake Facebook Site

SnapChat

kik

Aaron Couch
Gah! My stupid boss! I swear, I hate him.

Scam

Keep personal information personal

Never post when angry

Things are not always as they seem

Be cautious with apps

Time Remaining
00.59

The threat of online predators

Don't communicate with strangers

Special Comment(s): . Drag the text on the correct picture box. For a correct try "Awesome guess!" and for incorrect try " Good attempt! Try Again!" is displayed. (Audio voice will also be used at each feedback). The user can have two maximum chances, failing in which the correct answer is displayed on the screen. No marks awarded for this activity. At the completion of the activity learners are awareded with a badge.

Figure 4.10 Drag and Drop Activity Lesson 1

Page Title: **ACTIVITY: Quiz- Sharing Privacy online**	Page no. 00.06.03.00	SME's name:
Date Designed:		Date verified:

Design

Special Comment(s): The next button is disable until the answer is attempted. Each correct attempt the learner will earn a star.

1. Sureni has been talking online to a girl named Tasha for a few days now. Tasha has told Sureni where she lives, how old she is, where she goes to school, and what she looks like. Tasha asks Sureni what school she goes to.

Is it okay for Sureni to tell her?

○ Yes, it is okay **(Good try! Try Again!)**

○ No, it is a bad decision **(Great! Your answer is correct, It's not a good decision, because the name of Sureni's   school is a personal information and she doesn't really know who is Tasha to reveal her information.)**

2. Lina receives an E mail stating that she has won a $1000000 lottery for which she has never participated and asks her to fill an online form using her personal information and credit card number to get the registration in order to receive the money.

What type of mail has she received?

○ Genuine mail **(Good try! Try Again!)**

○ Phishing mail **(Great! Your answer is correct, It is a phishing mail because it's a lottery ticket which she has never participated)**

○ Fake mail **(Good try! Try Again!)**

3. Lashan has visited a particular website through his Facebookaccount to download one of his favourite games. His friend Akila has told him that Lashan's profile detail would be recorded in the server of the webiste's company. Lashan is worried now.

How does this happen?

○ because the company has a software to hack the details **(Good try! Try Again!)**

○ The company website has super cookies which can save his data automatically **(Great! Your answer is correct, Because a super cookie is hard to delete and cookies will create a copy of the viewer's details)**

○ The company website may send a virus to track his details **(Good try! Try Again!)**

4. If someone online tells you they are in 6th grade and their name is Katie, they are probably how old?

  ◯12 years (**Good try! Try Again!**)

  ◯13 years (**Good try! Try Again!)**

  ◯35 years (**Good try! Try Again!)**

  ◯There's no way to tell (**Great! Your answer is correct, High risk of guessing correctly, there's no way to tell**

5. If you have been talking on the Internet to a person for a long time, and they want to meet, which is okay to do?

  ◯ Meet them, as long as you bring a friend (**Good try! Try Again!**)

  ◯Meet in a public place. (**Great! Your answer is correct, Better to meet in public**)

  ◯Tell someone where you will be before you go.(**Good try! Try Again!**)

  ◯Ask your parent or guardian first and have them go with you.(**Good try! Try Again!**)

6. It is okay to send someone online your picture when:

  ◯They send you theirs first (**Good try! Try Again!**)

  ◯ You send them an old picture (**Good try! Try Again!**)

  ◯
    As long as you don't send them your address too (**Good try! Try Again!**)

  ◯ Only if a parent or guardian is with you and says it is okay (**Great! Your answer is correct, Better to meet in public**)

7. Shaneli is a 10 year old girl. She has started to chat with an online friend who seems to be very pleasing and pleasant. However, one day Shaneli's parent's revealed that the partner whom she was chatting had had a sexual misconduct verbally with her and immediately stopped her use of chatting.

What type of sexual contact does Shaneli has come across in the cyberspace?

  ◯ sexting (**Good try! Try Again! this means sending sexual photos to others**)

○ stalking (**Good try! Try Again! this means making you scared/ stalked**)

○ grooming (**Great! Your answer is correct, this means a gradual approach to sexual misconduct**)

○ harassing (**try! Try Again! this means making you violently harassed**)

8.   If you have received an e mail from an unknown friend, can you check his/her profile and trust that information?

○ True   (**Good try! Try Again!**)

○ False (**Great! Your answer is correct, it is probable to be a fake profile**)

Figure 4.11 Quiz Activity Lesson 1

Page Title: **ACTIVITY: Activity-Quiz Summary**	Page no. 00.06.04.00	SME's name:
Date Designed:		Date verified:

Design

| Special Comment(s):   Summary will display the calculated marks, date, time and status. Mark is awarded out of 10 only for this activity. As this is an awareness course the marks are not carried as a final mark. Completion and achievement rewards are encouraged.

Ref: file 101 to get the background picture for this particular screen. |
|---|

Figure 4.12 Summary of the Quiz Activity Lesson 1

Storyboard-Post Activity on Cyber Dating

Page Title: **ACTIVITY: Post- Activity- Cyber Dating**	Page no. 00.08.03.00	SME's name:
Date Designed:		Date verified:
Design		

Special Comment(s): This activity has to be created as a drag and drop game. The given boxes have to be dragged and dropped to the correct blank. The audio button is provided for the learners to listen to the story which is based for filling the blanks. The content of the audio will be provided below.

Each correct attempt the learners will hear an applause sound and each wrong attempt learners will hear try again…

Figure 4.12 Online Dating Activity Lesson 1

Chapter 5: Development and Implementation

5.1 Introduction

This chapter gives the reader a full account of how the online course was built. Many software tools were used to design the course content. The content was developed using text, graphic, animations, audio and video features. The learners are of different learning abilities and that was particularly considered when using the tools. The content has been developed to suit the different types of learners. The learner can choose the mode of the lesson that suits him/her well.

SCORM standards were used whenever possible. SCORM has many advantages as it can support many different type of third party software, which can be bought for readymade.

Most of the lessons compromises animated and real videos, which require a considerable bandwidth, therefore in order to have a better performance, the videos are developed and uploaded to the you tube and only the links are provided in the LMS.

Each module is contained with a lesson video or interactive slideshow and post quiz activity or a game. Some of the quizzes are developed in the LMS and some others are constructed through Xerte tool and java scripts. The whole course was uploaded to the Moodle based LMS. Some of the content of the course is build with the embedded tools in Moodle and most of the others are done using the third party tools. Such as, movies I have been recorded and edited on my own in Premier and lesson videos are made using free online animated software.

5.2 Development Process

The ADDIE model was used as the Instructional Design Methodology to proceed with the process of the development life cycle of the project.

Phase	Step	Purpose	Activities	Deliverables
Analysis	Analyzing	Identify the problem	Analysis stage activities	Refer the Chap 3 Planning and Analysis
Design	Design the content	Blueprint of the system to be developed	Course Map, Syllabus, Storyboards	Refer the Chap 4 Design
Development	Developing the content material	Using different types of tools to develop the content	Real output is constructed	Ref Chap 5 Development
Implementation	Hosting the system online	Implement the system	Hosting, domain	Chap 5
Evaluation	Is the system successful or not	Evaluate the system	Evaluation criteria	Chap 6

Table 5.1 Development process of the cyber safety course

The Development of the process can be further explained in detail as follows:

In order to develop the content the most important part is selecting the LMS. In order to have a successful implementation in e learning the LMS should be fairly rich with the technological features which help to integrate the pedagogical approach.

5.3 Why Moodle has been chosen as the best LMS to be used?

The first and foremost thing is that Moodle is the open source system, which was used as a (LMS), for managing e learning materials. With customizable management features, it is used to create web sites for learning materials to achieve goals of the course. Moodle is very suitable for managing multimedia contents and has a good and relatively simple mechanism for tracking participants' activities. Further, the e learning advisors mentioned to use Moodle tools such as Forums, chat rooms, notifications, mailing lists, etc.

The storyboards were created in the design stage as the first draft material of the course content. Therefore based on the designed content the course was developed using the following tools,

Xerte tool

Open source tools for e learning developers and content authors producing interactive learning materials. E learning materials can be authored quickly and easily using browser-based tools, with no programming required. Xerte Online Toolkits is aimed at content authors, who will assemble content using simple wizards. Content authors can easily collaborate on projects. Xerte Online Toolktis can be extended by developers using Xerte.

Adobe captivate 8

Adobe Captivate is a rapid responsive authoring tool that is used for creating e learning content such as software demonstrations, software simulations, branched scenarios, and randomized quizzes in Small Web Formats (.swf) and HTML5 formats. This tool was very effective as it helped to create interactive slideshow presentations, drag and drop activities and many more interactive activities, which can be exported to LMS as SCORM packages which could be reusable.

71

Moovly POWTOON

It is a free online tool used to create interactive movie files or slideshows. The drawback is that its advance features are available for premier membership, which costs money. Other features of the software can be used to create a video with basic functionalities.

Word files

To type the content of the lessons

Adobe Premier

Though Adobe is not an open source tool, it is used to create and edit movies with high quality. It is very useful to create real live videos with minute alteration possibilities than Movie Maker.

Movie Maker

MOODLE version 3.0.4+ was installed successfully to the machine and configured in preparation for hosting the course. The course layout was developed in MOODLE as a draft version. MOODLE features were used for quizzes and assignments.

The course content was developed with video, slideshow lessons, Assessments including MCQ quizzes, drag and drop activities, etc.

5.4 The Developed content
Lesson on Cyber Dangers

Figure 5.1 Example 1 of developed content

This lesson is developed using Powtoon tool. Audio music and narration is provided for the learner. If the narration or music is not needed they can mute it. A video link will be provided in the LMS to overcome the network delays due to large amount of users at the same time.

Movie on Cyber Dangers
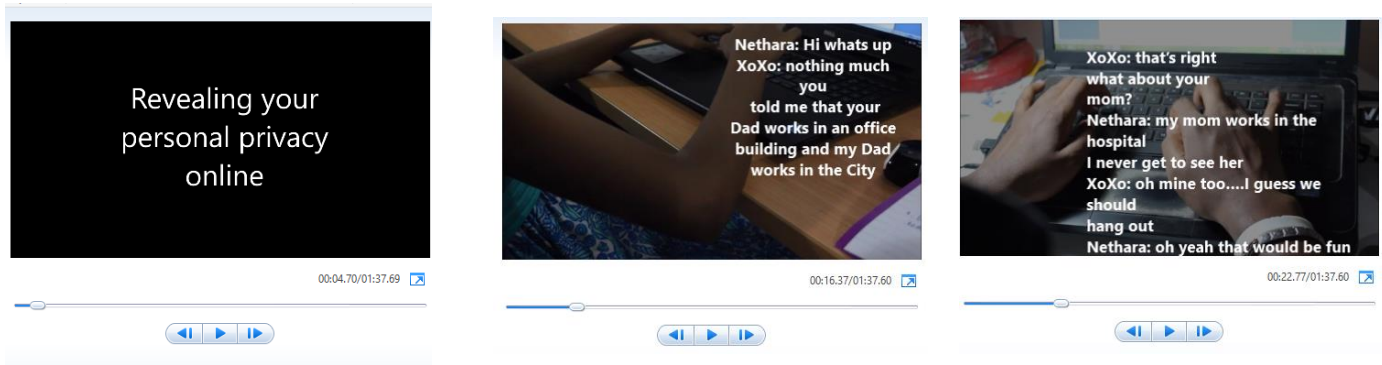
Figure 5.2 Movie on cyber dangers

These are few screenshots of an introductory movie for the dangers of revealing of personal information online. This has been developed using Adobe premier and live characters were used and televising was done by the author.
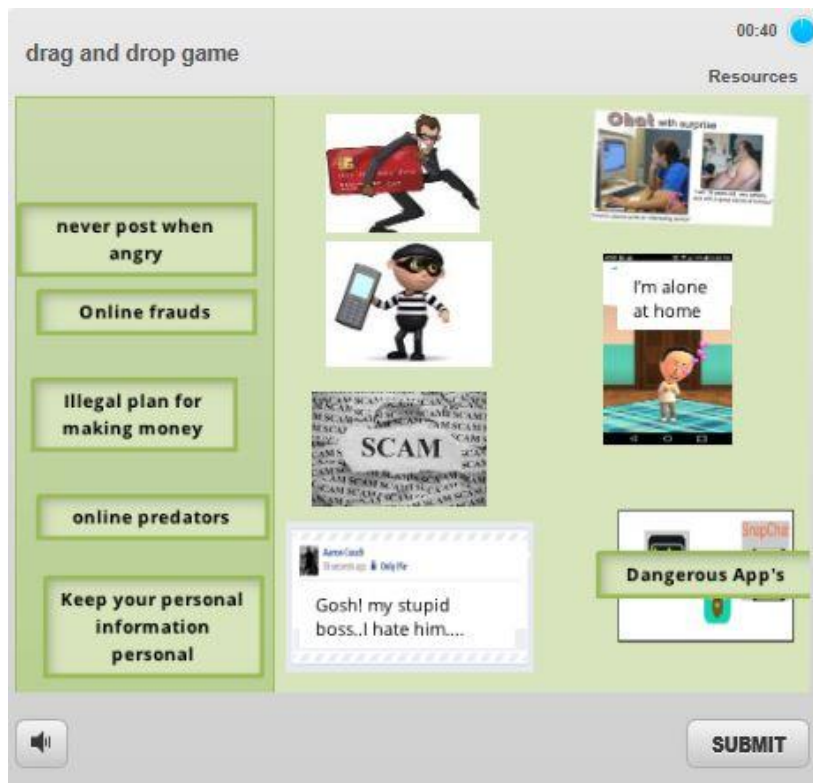
Figure 5.3 Drag and Drop Activity

Video-Personal Privacy

Figure 5.4 Video on importance of Personal Privacy

Pre-Activity- Online Dating
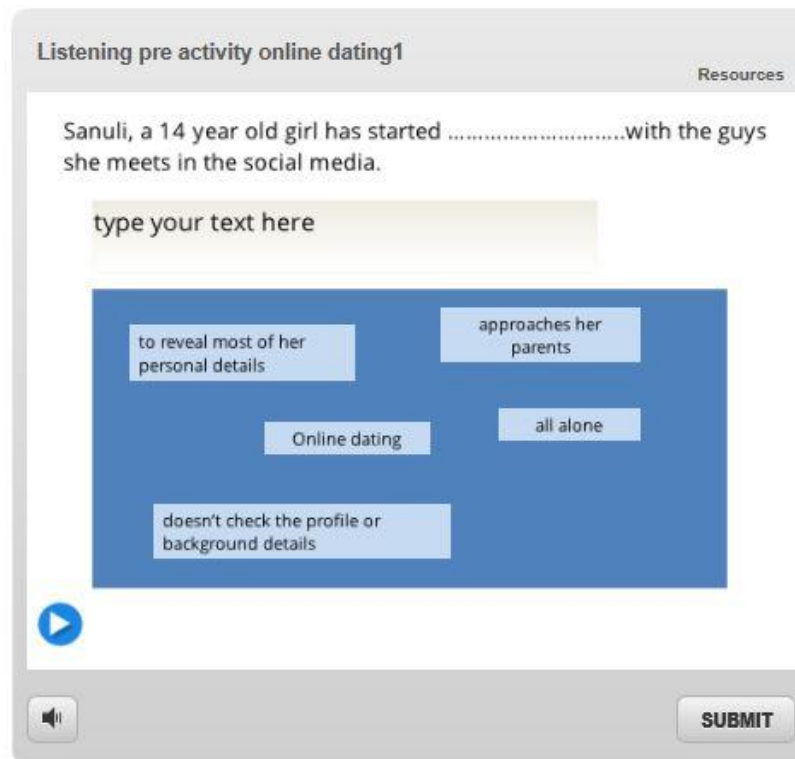
Figure 5.5 Pre Activity Online Dating

Quiz-Cyber bullying
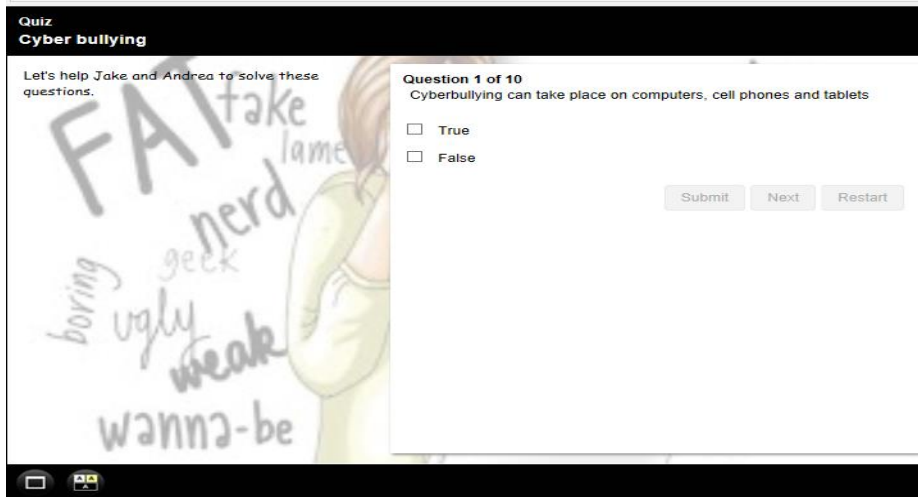
Figure 5.6 Quiz

Game- Treasure Hunt on Online Reputation

Figure 5.6 Treasure hunt on Online Reputation

This quiz has been created using Xerte tool which checks the knowledge of the learner on Cyber bullying.

5.5 Course Expectations

- The Cyber Safety course was primarily designed expecting an attitude change in the leaner at the end of the course with related to the cyber contacts when using the Internet.
- A new syllabus was designed for the proposed system and the following topics were included in the syllabus:

    1. Dangers of Cyber Contacts
    2. Online Reputation
    3. Copyright Infringements
    4. Addiction to Digital Media
    5. Balancing online and offline
    6. Online bullying and negotiation
    7. Psychological impact of online usage
    8. Healthy digital citizen

- Out of these topics, the topics below were able to cover for the course. The main course topics such as Cyber bullying, online reputation, dangers with Cyber contacts, digital addiction and psychological impact of online usage were able to successfully cover in the course.
- Some of the topics were not covered as the topics were given less priority. The target audience was most focused to give knowledge about self awareness on how to protect from cyber dangers. Further, a considerable time was taken to the development as most of the software tools were not familiar to the developer and as there was no proper concrete structured materials was not available for the course content, it took a long time to develop the content .

Chapter 6: Evaluation

6.1 Introduction

The post course evaluation offers you to check the interaction of the learner in the insight of the course.   This chapter reveals the Learner's participation and reaction to the learning content and how much they have absorbed or learnt from the content. Mixed method where, qualitative and quantitative was used to gather data in the questionnaire. The evaluation was done by a sample group of students and a questionnaire was used for the evaluation.   The feedback was taken on the quality of the course, effectiveness and relevancy of the course content, activities and assessments.   The questionnaire used for the evaluation is included in the appendix.

6.2 Analysis of Student's Feedback

The student feedback was taken under different categories. Each section was designed to evaluate different aspects of the course.

a) Visibility, system status and content

b) Course content

c) Course impression

The objective of evaluating the overall experience is to see whether the course met the user's Goal and objectives, whether the course was in line with the expectation of the user and whether the constructive alignment was found in the course.

6.2 Evaluation Process

The evaluation was done in two steps. First a questionnaire was distributed for the students who took part in the evaluation. Based on the results of the questionnaire the analysis indicated variety of results as discussed in the evaluation chapter.

Second step was on site observations, where the students were given to use the course in the school lab and observed whether the students have used the course content as expected and whether it achieved the aligned objectives of the course.

In the questionnaire the respondents were given to indicate whether they Strongly agree(SA), Agree(A), Strongly Disagree(SD), Disagree(D) and also was given the choice to state not applicable(NA) for statements which are not applicable. [Appendix A]

a)Visibility, system status and content

	SA	A	D	SD	NA
The interface of the online course is pleasant and attractive.	75%	25%			
Font size, style and colour are easy to read	80%	20%	-	-	-
Rate whether the guidelines of the course help you to safeguard yourself from cyber dangers	25%	75%	-	-	-
It is easy to navigate the course content	8%	90%	-	-	2%

Table 6.1 Evaluation 1

Majority of them stated that the course was helpful for them to safety decisions when using the Internet. Almost all the students agreed with the font size and appearance of the Interface. According to the respondents' feedback, it is understood that the course was constructively aligned.

b) Course Content

This section was used to help evaluate the user satisfaction with related to relevancy, clarity and effectiveness in the course content.

Course Content and Activities					
	SA	A	D	SD	NA
The audio and video were very useful to gain a clear understanding	80%	20%	-	-	-
The materials were interesting and engaging.	25%	75%	-	-	-
The materials were accurate and current.	80%	20%	-	-	-
The course activities helped me learn.	10%	80%	-	-	10%
Both novice and expert users can use it without any difficulty	75%	25%	-	-	-
All the course activities and quizzes were very well timed.	-	80%	-	-	-
Did you need to obtain additional material to complete the course? Yes ___ No ___ If so, what material or resources did you need?					
Were sections of the course especially difficult or confusing? Yes ___ No ___ If yes, please note what they were and explain why they were difficult or confusing?					

Table 6.2 Evaluation 2

The feedback of this section indicated that the course content activities were engaging, interactive, effective, clear, understandable and accurate. They were satisfied with the activities provided and it was revealed that they accept these activities are realistic and relevant.

However, some of the activities seem to be too easy and some were difficult for them. The feedback of this unit reveals that the assessments were designed with accuracy, relevancy and clarity. Also it was stated that they did not feel a test environment trying the activities and it was more fruitful for their understanding.

c) Final Impression about the course

This section allowed the user to answer an open ended question to get the feedback of suggestions to improve the course.

Final impression of the course
How could the institution improve the course and the online services it provides to students?

Table 6.3 Evaluation 3

The user mainly suggested adding more game based content to the lessons. Games such as race games, treasure hunt etc...

Chapter 7: Results and Discussion

7.1 Introduction

This chapter includes the evaluation process, a discussion on results; whether the results have proven that the course objectives are achieved and a discussion of results with similar online courses.

7.2 Results Discussion

The achievement of the objectives can be analysed based on the results of the evaluation.

7.2.1 Analysis of the Objectives

- **Objective 1-** To develop an adaptive online learning environment based on their level of knowledge within one year.

According to the first evaluation method, an evaluation questionnaire was provided for the students to compare their increase of awareness with the findings that was taken before the course implementation.

Compared to the results [Refer Appendix A] which were received in the analysis stage is considerable different from the results which were received in the evaluation stage. After following the course modules, about 85% of the children have achieved awareness on the danger behind saying true details to the strangers online and how to use their privacy online. Further they have identified the adverse effects of online games and the importance of limiting it. [Refer Appendix A]

About 75% of students have strongly agreed and 25% have agreed that the course interface is easy to be used by even a novice user. [Refer Appendix a Table 6.2]

Further about 80% agreed that the course is well suited for their level of knowledge. Thus the first objective has been achieved approximately 75%.

- **Objective 2**- To develop a standard curriculum which supports the learners to arouse or increase the awareness on the risks and threats of the online environment.

  A curriculum was developed successfully for a period of one year [Appendix B]. This curriculum has increased the awareness on the risks and threats. According to the results of evaluation, about 75% of students admitted that the guidelines of the course have helped to safeguard themselves from the Cyber dangers. Further, 80% of them have found the activities very much helpful for them to increase the awareness related to the subject. [Refer Appendix a Table 6.1 and 6.2]
  Thus, the second objective has been achieved.

- **Objective 3-** To promote learner motivation by introducing interactive activities and reward schemes such as, badges /certificates.

  Learners were awarded with a badge at the end of quiz activities in order to motivate them to follow the course. As a result 75% of students have admitted that they were motivated to try the quizzes with interest to achieve the badges. Thus, the learner motivation has been increased and the course objective has been achieved. [Refer Appendix a Table 6.2]

Thus, it can be assumed that the Goal to mitigate the unhealthy behaviour of the Middle school students with the use of digital devices by introducing a virtual learning system has been successful.

Further, evaluating whether the Instructional objectives are achieved or not in each lesson module a separate questionnaire was provided based on each module's learning outcome. In the questionnaire the respondents were given to indicate whether they Strongly agree(SA), Agree(A), Strongly Disagree(SD), Disagree(D) and also was given the choice to state not applicable(NA) for statements which are not applicable. [Appendix B]

Lesson 1- Dangers of Cyber Contacts					
	SA	A	D	SD	NA
Able to list different types of dangers of Cyber contacts with the help of videos, activities and quizzes.	80%	20%	-	-	-
Able to interpret the ideas effectively using discussion forums	-	50%	10%	-	40%
The quizzes drag and drop activities and other resources helped me to apply the knowledge and construct solutions for real life scenarios.	80%	20%	-	-	-
Were sections of the course especially difficult or confusing? Yes ___ No ___ If yes, please note what they were and explain why they were difficult or confusing?					

Table 7.1 Results Discussion on Lesson 1

Based on the table above it is identified that the course materials has successfully aligned with the objectives in the module 1. However, it seemed that use of the discussion forum was not effective as expected as students took a long duration to post comments and they could not make it a productive communication.

Lesson 2- Online Reputation					
	SA	A	D	SD	NA
Able to define Online Reputation and its positive and negative behaviours with the help of videos, visual images, lessons and resources	80%	20%	-	-	-
The videos and guidelines helped you to understand and act correctly when interacting with online.	10%	80%	-	-	10%
Able to share the work with other group of friends and learn more.	80%	20%	-	-	-

Table 7.2 Results Discussion on Lesson 2

Based on the table above it is identified that the lesson objectives have been successfully aligned with the course content and the learners have gained satisfaction with the activities designed.

Lesson 3- Cyber bullying					
	SA	A	D	SD	NA
Able to define and state the consequences of Cyber bullying with the help of the movies, videos and resource materials.	20%	80%	-	-	-
Able to act out any time to prevent Cyber bullying in school or outside with the help of the tips and guidelines provided in the course.	10%	80%	-	-	10%
The quizzes and guideline materials helped me to practice netiquette in collaborative online communication	20%	80%	-	-	-

Table 7.3 Results Discussion on Lesson 3

The lesson objectives have been achieved up to an extent. The learners have become motivated to follow the guidelines at least during the use of the collaborative activities.

Lesson 4- Digital Addiction					
	SA	A	D	SD	NA
Able to become aware on different types of addiction and its consequences with the help of documentaries, videos and visuals.	20%	80%	-	-	-
Quizzes and Interactive activities helped to recall the symptoms and effects of Online Addiction.	40%	60%	-	-	-
Able to interpret ideas on what you learnt about digital addiction with the help of forums and sharing activities	10%	80%	-	-	10%

Table 7.4 Results Discussion on Lesson 4

Based on the table above the lesson objectives are successfully achieved and aligned with the objectives.

Lesson 5- Psychological impact of digital use					
	SA	A	D	SD	NA
The interactive lessons and shared links on the Internet helped you to remember and recall the psychological effects of the overuse of the Internet.	-	90%	10%	-	-
Quizzes and offline activities have helped me to understand the danger behind psychological impact of the overuse of the Internet	40%	60%	-	-	-
Was this lesson helped to realize the negative consequences of digital addiction in a more better way		85%	5%	-	10%

Table 7.5 Results Discussion on Lesson 5

Based on the above diagram, it is identified that the learners have been able to list psychological effects of digital overuse and construct solutions to any given scenarios.

Lesson 6- Internet Safety and Reporting Crime					
	SA	A	D	SD	NA
Able to apply the knowledge on preventing from fake profiles and safeguarding yourself with the help of the tips on cyber wellness lessons and resources.	10%	90%	-	-	-
The visual pictures, you tube video links and quizzes helped you to learn how to make decisions when surfing online	40%	60%	-	-	-

Table 7.6 Results Discussion on Lesson 6

Overall all the course contents helped me to create a sound awareness of Cyber Safety to mitigate the unhealthy relationships with the online in day today life.	30%	70%	-	-	-

Table 7.5 Results Discussion

Overall the course has met the expected objectives and has achieved constructive alignment in each module. However, there are limitations too that have been identified when compared with similar online courses.

Questionnaire on evaluating the course content with the objectives

	SA	A	D	SD	NA
Able to list different types of dangers of Cyber contacts with the help of videos, activities and quizzes.					
Able to interpret the ideas effectively using discussion forums					
The quizzes drag and drop activities and other resources helped me to apply the knowledge and construct solutions for real life scenarios.					
Were sections of the course especially difficult or confusing? Yes ___ No ___ If yes, please note what they were and explain why they were difficult or confusing?					

Table 7.6 Results Discussion on course content

Chapter 8: Conclusion and Future work

8.1 Introduction

This chapter includes concluding remarks about the project and its development process. It also includes the future developments.

8.2 Conclusion

The e learning theories were put into the practice by the author and an e learning framework was successfully constructed using the knowledge of the author encountered with related to multitude of concepts, strategies and theoretical approaches of e learning.

Vast number of e learning tools was used in developing the course and it has enriched not only the course but also the author as well. Learning, exploring and experimenting was challenging but it's rewarding as it will pave the way to future projects.

The Cyber Safety course will open avenues for the Schools to introduce the threats and risks of the Internet to children as well as ways to safeguard them. The children can experience videos, audios and lesson oriented games to learn the risk of the internet. At present local or international schools in Sri Lanka lacks a proper syllabus to be followed in the school about Cyber Safety and therefore, the said course will be a good solution to enhance the knowledge of the children and create awareness among them. In this course children will be able to playfully engage in the activities and lessons not as an exam oriented subject. The speciality of the course is that the user can enrol for free and have an experiential learning about how to safeguard them on the Internet.

8.3 Future Developments

The success of the course stands to validate the viability of this framework; hence this project would lead to further investigations. The success of the course is to validate the viability of using Cyber Safety guidelines in the user's day today life. Further, a parent's access also will be added to the e learning coursework as parents too need to be aware to protect their children from these threats.

References

[1]A. Lenhart, K. Purcell, A. Smith and K. Zickurh, "Social Media and mobile Internet use among teens and young adults.", Pew research center, Washington, DC, 2010. [Online]. Available: http://LENHART, A., PURCELL, K., SMITH, A. AND ZICKUHR, K.

[2]A. Beale and K. Hall, "Cyberbullying: What School Administrators (and Parents) Can Do", *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, vol. 81, no. 1, pp. 8-12, 2007.

[3]E. BURGESS DOWDELL, "Risky Internet Behaviors of Middle-School Students", *CIN: Computers, Informatics, Nursing*, vol. 29, no. 6, pp. 352-359, 2011.

[4]"The Teacher's Guide to Keeping Students Safe Online - eLearning Industry", *eLearning Industry*, 2013. [Online]. Available: https://elearningindustry.com/the-teacher-guide-to-keeping-students-safe-online.

[5]"Fighting Cyber Crime | The Sunday Leader", *Thesundayleader.lk*, 2017. [Online]. Available: http://www.thesundayleader.lk/2015/06/21/fighting-cyber-crime/. [Accessed: 08- Jun- 2017].

[6]"Home", *Telligp.police.lk*, 2017. [Online]. Available: http://www.telligp.police.lk. [Accessed: 08- Jun- 2017].

[7]"Homepage - Netsafe: Supporting New Zealand internet users", *Netsafe: Supporting New Zealand internet users*, 2017. [Online]. Available: http://www.netsafe.org.nz. [Accessed: 08- Jun- 2017].

[8]"Main Page", *FBI*, 2017. [Online]. Available: https://sos.fbi.gov. [Accessed: 08- Jun- 2017].

[9]"Sexting", *Office of the Children's eSafety Commissioner*, 2017. [Online]. Available: https://www.esafety.gov.au/esafety-information/esafety-issues/sexting. [Accessed: 08- Jun- 2017].

Appendix A – Descriptive Analysis

Table 01: composition of the sample by the mode of accessing internet

mode of accessing internet	count	percentage
Parent's guardian's computer at home	6	12
Own laptop	7	14
Mobile phone	35	70
Internet café	1	2
Other	1	2
	50	100

Figure1: composition of the sample by the mode of accessing internet
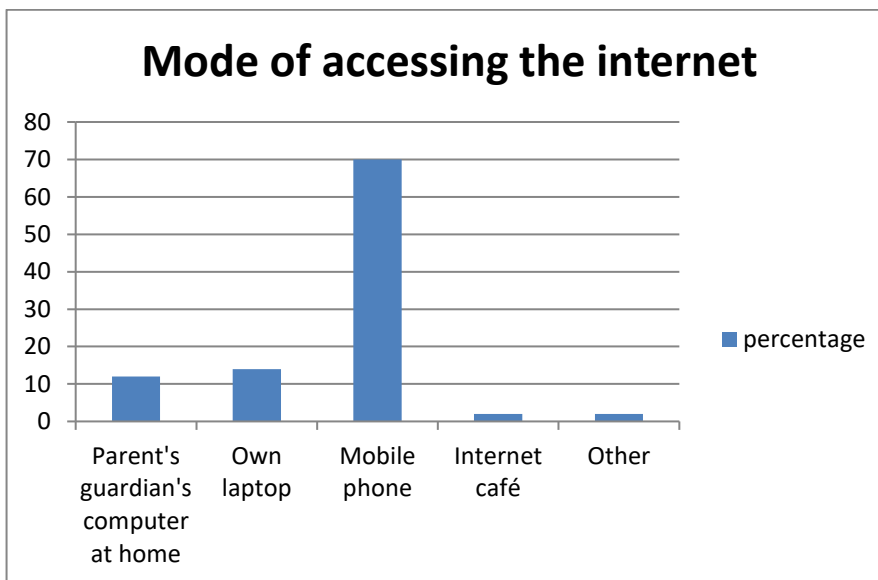

In the sample, a vast majority of 70% of the students are accessing the internet by the use of a mobile phone. The second most method of accessing the internet is through their own laptop which is about 14%. 12% of students use parent's guardian's computer. And only about 4% of the students use Internet cafes or other modes to access internet.

Table 02: composition of the sample by the usage of internet on weekdays

number of hours spent on the internet on week days	count	percentage
0	2	4
1	5	10
2	6	12
3	10	20
4	11	22
5	16	32
	50	100

Figure 02: composition of the sample by the usage of internet on weekdays
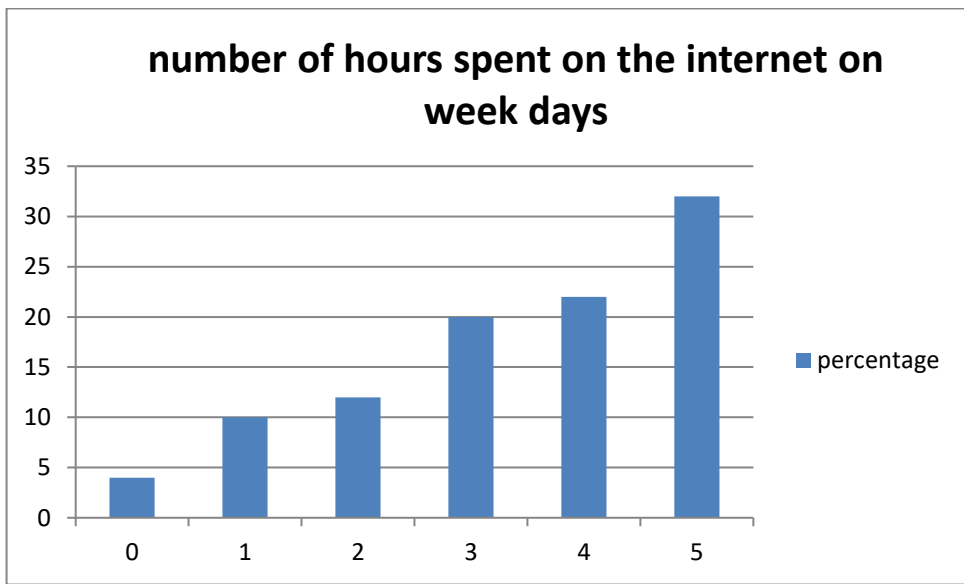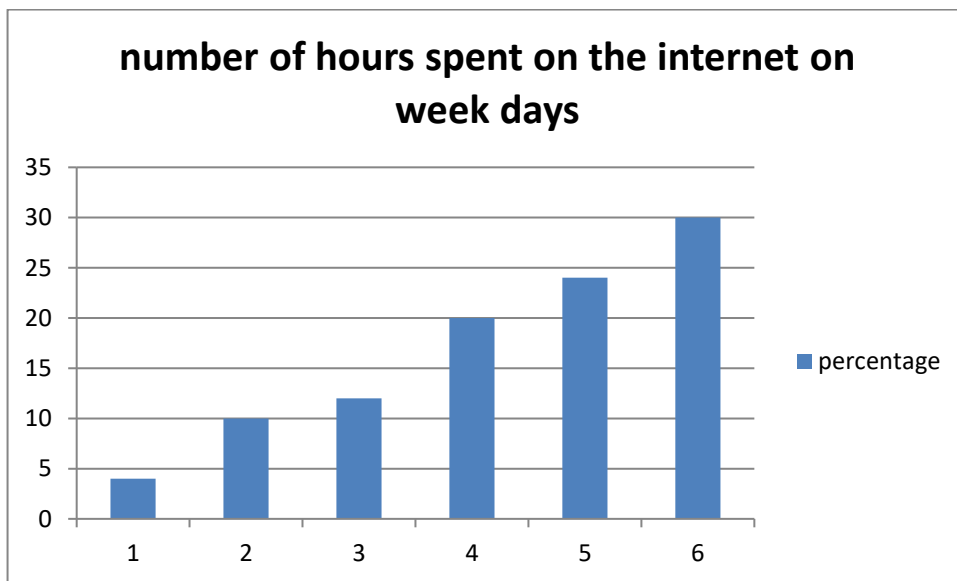

In the sample, a 32% of the students use the internet for five hours on weekdays, 22% of the students use the internet for four hours, 20% of the students use the internet for three hours and 12% uses for two hours, 10% of students for 1 hour and 4% of students do not use the Internet on weekdays.

Table 3: composition of the sample by the usage of Internet on weekends

number of hours spent on the internet on week days	count	percentage
1	2	4
2	5	10
3	6	12
4	10	20
5	12	24
6	15	30
	50	100

Figure3: composition of the sample by the usage of Internet on weekends


In the sample 30% of students use the Internet for 30 hours, and averagely 20% and 24% of students use the Internet for 4 and 5 hours respectively. 10% and 12% of students use internet for 2 and 3 hours respectively, while 4% of students use only an hour on the Internet.

Table 04: Composition of the sample by the social network sites visited

Social network site	Count	Percentage
Facebook	35	70
Twitter	12	24
Instagram	25	50
Snapchat	16	32
WhatsApp	38	76
other	20	40

**Figure 04: Composition of the sample by the social network sites visited**
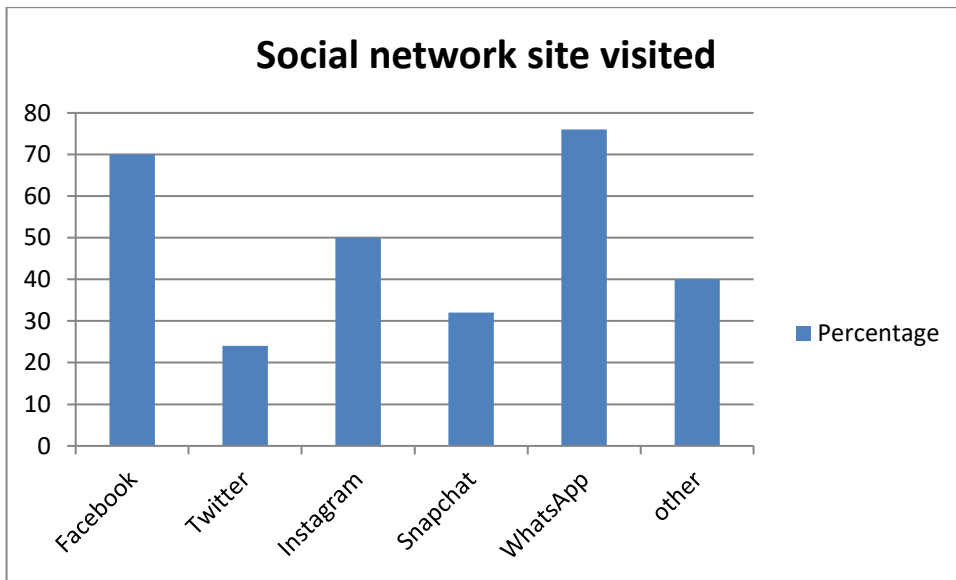
About 76% of the students visit WhatsApp and 70% of students use Facebook. About 50% of the students visit Instagram. 32% of the students use snapchat.

Note : According to Question 6 in the questionnaire, all the students use social Networking media.

Table 05 : composition of the sample by the opinion of cyber threats

type of threat	Count	Percentage
bullying/harassments	12	24
unwanted sexual approaches	11	22
coming across sexual content	10	20
using photos inappropriately	17	34
	50	100

**Figure05: composition of the sample by the opinion of cyber threats**
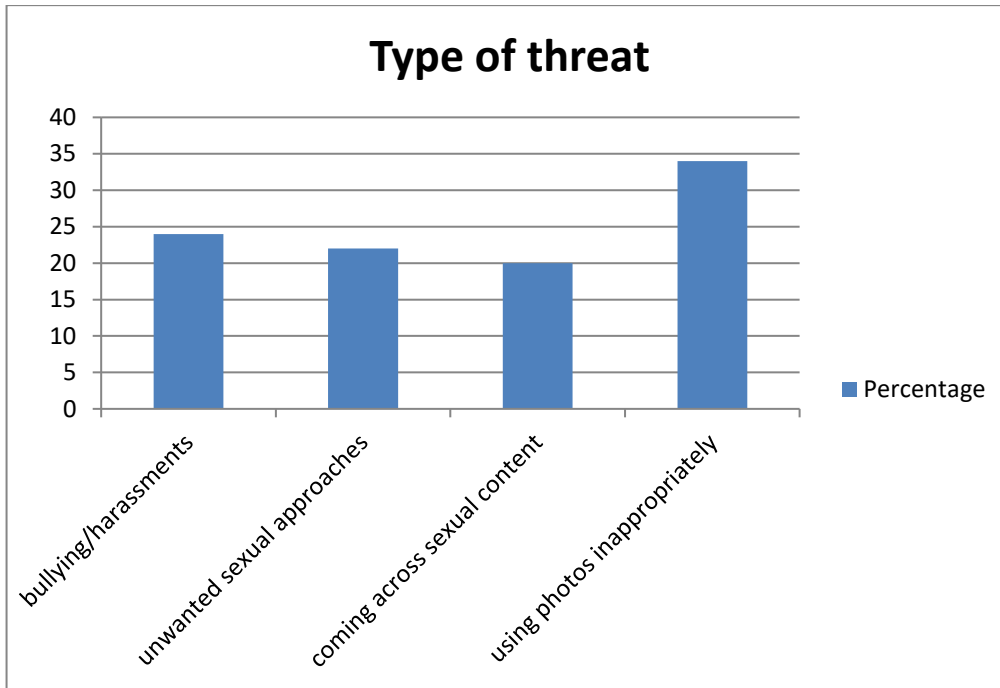
34% of the students consider sexting photos inappropriately as the biggest threat using the internet, while 24% of the students consider bullying as the biggest threat. Coming across sexual content is considered as the biggest threat by only 20% of the students.

Table 08: Composition of the sample by the number of the times the students have revealed their personal details online

Number of times they have revealed their true personal details online	count	percentage
0	5	10
1	3	6
2-5	12	24
more than 5	30	60
	50	100

Figure 08: Composition of the sample by the number of the times the students have revealed their personal details online
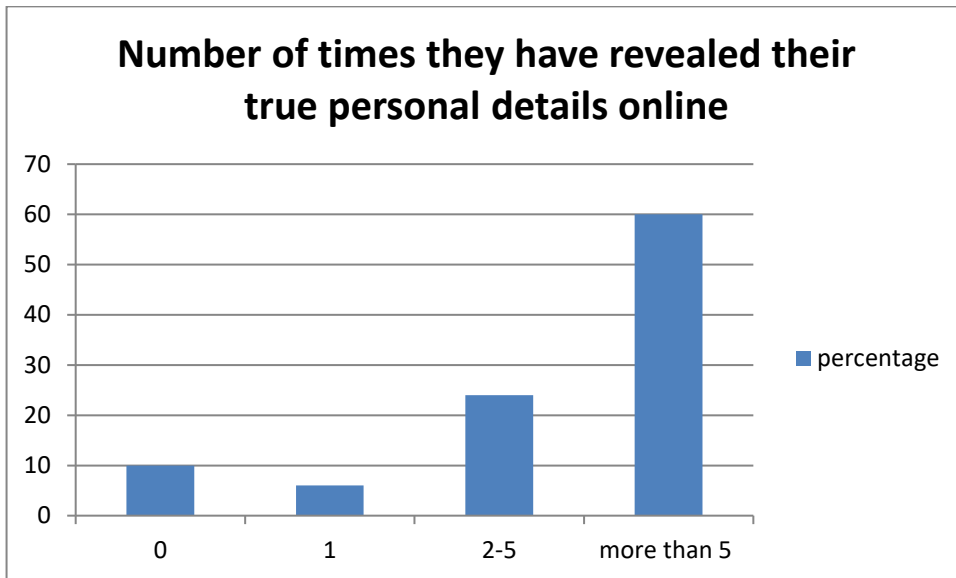
40% of students have revealed their true details twice in their usage, while less than 15% of students have revealed their true details more than 5 times in their usage and around 28% of students have revealed their true details at once.

Table 04 : composition of the sample by awareness of privacy settings

Awareness or non awareness	count	percentage
aware of privacy settings	32	64
not aware of privacy settings	18	36
Total number of students	50	100

Figure4: composition of the sample by awareness of privacy settings
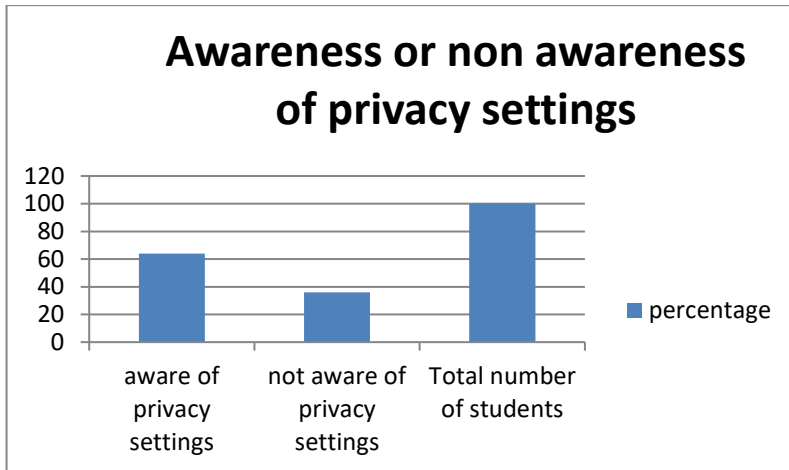
Almost 64% of the students are aware of the privacy settings, but a significant percentage of students about 36% are not aware of privacy settings

Table 05 : composition of the sample according to frequency of communication between parents and children about internet

Frequency of communication	Number of students	Percentage
Never	3	6
Rarely	9	18
Sometimes	20	40
Regularly	18	36
	50	100

Figure5: composition of the sample according to frequency of communication between parents and children about internet
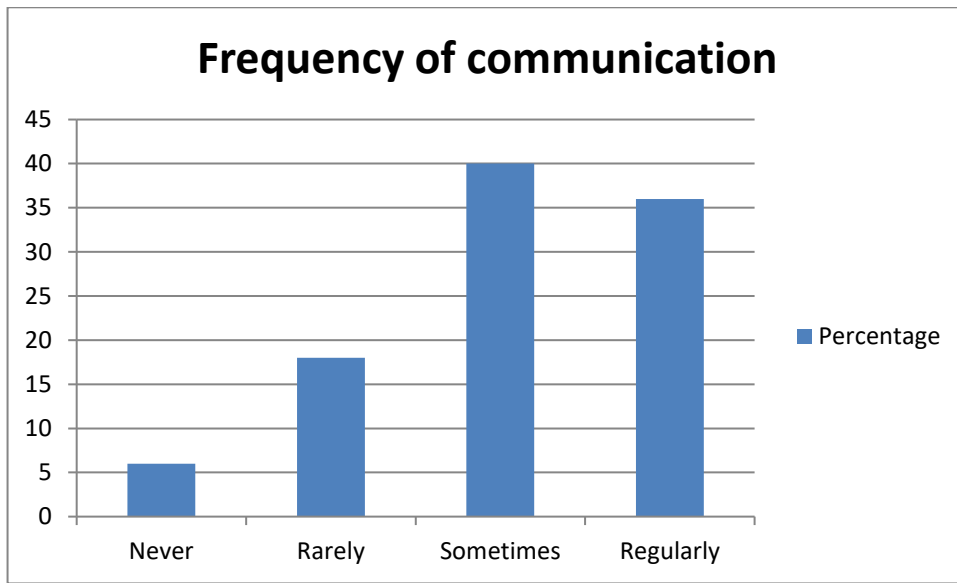
Only 36% of the students communicate regularly with parents. So the remaining 64% of the students do not engage in frequent communication with their parents.

Table 06 : composition of the sample according to level of restrictions regarding internet usage

Extent of rules regarding internet use by parents	count	percentage
No rules	17	34
Access restrictions	6	12
Time limits	26	52
Both access and time restrictions	1	2
	50	100

Figure 6: composition of the sample according to level of restrictions regarding internet usage
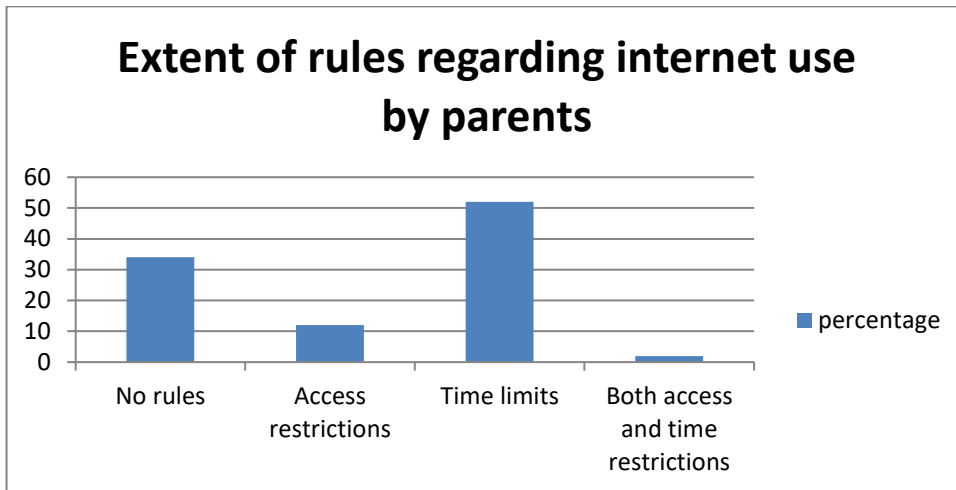
Extent of rules regarding internet use by parents

34% of the students have no restrictions imposed on their internet use by parents. Only 12% have access restrictions. A very low percentage of 2% only has both time and access restrictions imposed on their internet use.

Table 11: Composition of the sample by the knowledge on block or report options

know block options	20	40
don't know block options	30	60
	50	

Figure 11: Composition of the sample by the knowledge on block or report options
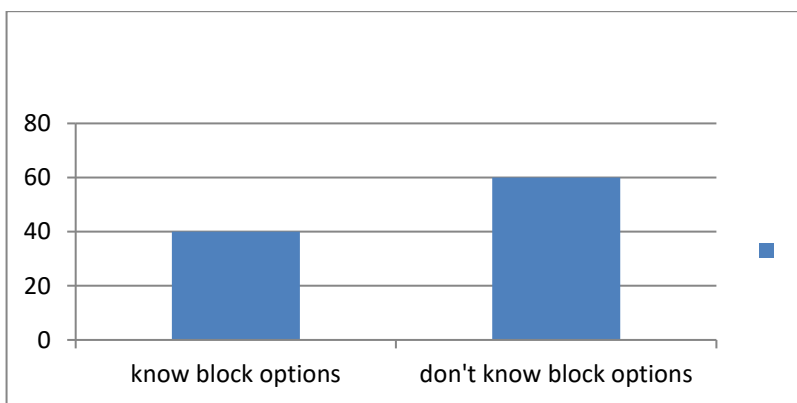
It is recorded that 40% of students seems to know block options when they use social networking or chatting and 60% of students do not have the knowledge on how to use the block options.

Table 12: Composition of the sample by the percentage playing online games

play online games	42	84
do not play online games	8	16

Figure12: Composition of the sample by the percentage playing online games

It is found out that more than 80% of students play online games, whereas less than 20% of students do not play online games.

Appendix B

Questionnaire for Analysis

male
13

Students e-Safety Survey

1. How do you access the internet? Please choose all that apply.

   Parent's/guardian's computer at home ☐

   Own computer at home ☒

   Own laptop ☐

   Mobile phone ☒

   Internet café ☐

   Friend's house ☐

   School ☐

   Other ☐

2. What do you use?

   Xbox ☐   Playstation ☒   PC ☒   Laptop ☐

   Tablet ☒   Nintendo Wii ☐

   Other ☒

3. Do you know how to use the privacy and security settings on these devices?

   Yes ☒   No ☐

1

9. Do you use social networking (If No, move to the next question)

Facebook ☐
Twitter ☐
Instagram ☐
Snapchat ☐
YouTube ☑
Skype ☑
Facetime ☑

Other   Please state any other.......................................

10.   What do you think is the biggest threat when you go online?

☑Bullying or harassments by friends or acquaintances

☐unwanted sexual approaches in a chat room, social networking site, email

☐coming across sexual images, content

☐someone is using my photo in an inappropriate way

☑someone taking my photo and circulating them

☐None of these

Please specify other ways

[   ]

11.   Do you know how to block and report on these social networks (if you use them)?

Yes ☑   No ☐

3

12.   Do you play online games?

Yes ☒   No☐

13.   When you are at school, do you know what to do or who to talk to if somebody says something hurtful to you online, or if something makes you feel uncomfortable?

Yes ☒   No☐

14.   How many times have you?

	0	1	2-5	more than 5
Added a stranger to the instant messenger contact list	☐	☒	☒	☐
Add a stranger to a social networking friend list	☐	☐	☒	☒
spoken on the phone to someone you met online	☒	☐	☐	☐
revealed your true personal details online	☒	☒	☐	☐

15.   As a girl/boy is there any specific issues you would like to share.

Nothing just many unkown people follow me.
After sometime
but I dont follow them back or they dont
they dont follow me.

Appendix C - Questionnaire for Evaluation

In an effort to evaluate the effectiveness and efficiency of the course Cyber Safety, I am seeking your feedback. I ask for your participation for evaluation purposes only. Also, the data you provide in the survey will not be used for, or in, any research and/or publications. All responses will remain private and confidential.

The survey will take 15-20 minutes of your time.

Visibility of the system status and content

1. The interface of the online course is pleasant and attractive.

    a. Strongly agree

    b. agree

    c. disagree

    d. Strongly Disagree

2. Font size, style and colour are easy to read

    a. Strongly agree

    b. agree

    c. disagree

    d. Strongly Disagree

3. .Rate whether the guidelines of the course help you to safeguard yourself from cyber dangers:

    a. Strongly agree
    b. agree
    c. disagree
    d. Strongly Disagree

4. Course materials are clearly and logically organized

    a Strongly agree

    b. agree

    c. disagree

    d. Strongly Disagree

5. It is easy to navigate the course content

a. Strongly agree

b. agree

c. disagree

d. Strongly Disagree

Course Content and Activities

6. The audio and video were very useful to gain a clear understanding

a. Strongly agree

b. agree

c. disagree

d. Strongly Disagree

7. The materials were interesting and engaging

a. Strongly agree

b. agree

c. disagree

d. Strongly Disagree

8. Both novice and expert users can use it without any difficulty

a. Strongly agree

b. agree

c. disagree

d. Strongly Disagree

Course impression

9. This course helped me to be a good digital citizen (helped me to take the correct decision when using online)

   a. Strongly agree

   b. agree

   c. disagree

   d. Strongly Disagree

10. Activities and facilities available in online course encourage student- teacher and student-student interaction (Forums, chat sessions, interactive activities and games)

   a. Strongly agree

   b. agree

   c. disagree

   d. Strongly Disagree

11. I am satisfied with the online course

   a. Strongly agree

   b. agree

   c. disagree

   d. Strongly Disagree

12. What are your suggestions for improvement of online course?
   i suggest the navigation of the website to be little bit easy, but this website is very educational.

13. To which extent online learning supports your overall learning.
   This website actully teached me about online dangers as a teenager that i can face.

THANK YOU

Appendix D

Ministry of Education (Malaysia)

https://www.moe.gov.sg/education/programmes/social-and-emotional-learning/cyber-wellness

Appendix E

Approval of the Newly compiled syllabus
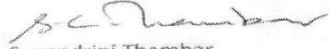

ASIAN INTERNATIONAL SCHOOL

13-09-2016

Director,
Postgraduate Division,
University of Colombo - School of Computing,
UCSC Building Complex,
35, Reid Avenue, Colombo 7,

Dear Sir,

Re: Cyber Safety Course for Middle School Students at Asian International School

As per the request made by Mrs. Nilma Weerasinghe (MIT SEM 3), I have approved the syllabus designed for the e learning course on Cyber Safety (which is to become a part of our Value Education & IT curriculum from 2017 onwards) as it is in accordance with the requirements of our school and on par with standards maintained in our institution.

Thank You,

Suvendrini Thambar
Head of Middle School & Student Services

Suvendrini Thambar
Head of Middle School

Director Consultant : Mrs. Goolbai Gunasekara - B.A., D.Litt.
Tel: 2512183
E-mail : goolbai@gmail.com

4/97, Thalakotuwa Gardens, Colombo 5. Tel : 2512182-3, 251 E-mail : asianinter@eureka.lk

98

Appendix F

Incident reported to Sri Lanka CERT |CC

Type of Incident	Year 2015
Phishing	14
Abuse/Hate/Privacy violation (via mail)	21
Scams	18
Financial Frauds	12
Malicious Software issues	10
Web site Compromise	20
Compromised Email	16
Intellectual property violation	3
DoS/DDoS	3
Social Media related incidents	2850
Total	**2967**

Type of Incident	Year 2014
Phishing	12
Abuse/Privacy	8
Scams	12
Malware	3
Defacements	56
Hate/Threat Mail	10
Unauthorized Access/Attempted	8
Intellectual property violation	3
DoS/DDoS	6
Fake Accounts/social media	2250
Total	**2368**

Type of Incident	Year 2013
Phishing	8
Abuse/Privacy	8
Scams	18
Malware	2
Defacements	16
Hate/Threat Mail	8
Unauthorized Access/Attempted	11
Intellectual property violation	3
DoS/DDoS	1
Fake Accounts	1200
Total	**1275**

Type of Incident	Year 2012
Phishing	8
Abuse/Privacy	8
Scams	6
Malware	2
Defacements	15
Hate/Threat Mail	6
Unauthorized Access	1
Intellectual property violation	3
DoS/DDoS	1
Fake Accounts	1100
Total	**1150**

Type of Incident	Year 2011
Phishing	6
Abuse/Privacy	2
Scams	3
Malware	1
Defacements	20
Hate/Threat Mail	3
Unauthorized Access	3
Intellectual property violation	5
DoS/DDoS	1
Fake Accounts	1425
Total	**1469**

Type of Incident	Year 2010
Phishing	6
Abuse/Privacy	20
Scams	10
Malware	5
Defacements	8
Hate/Threat Mail	12
Unauthorized Access	10
Fake Accounts	80
Total	**151**

Type of Incident	Year 2009
Phishing	10
Abuse/Privacy	10
Scams	11
Malware	12
Defacements	15
Hate/Threat Mail	8
Unauthorized Access	3
Total	**69**

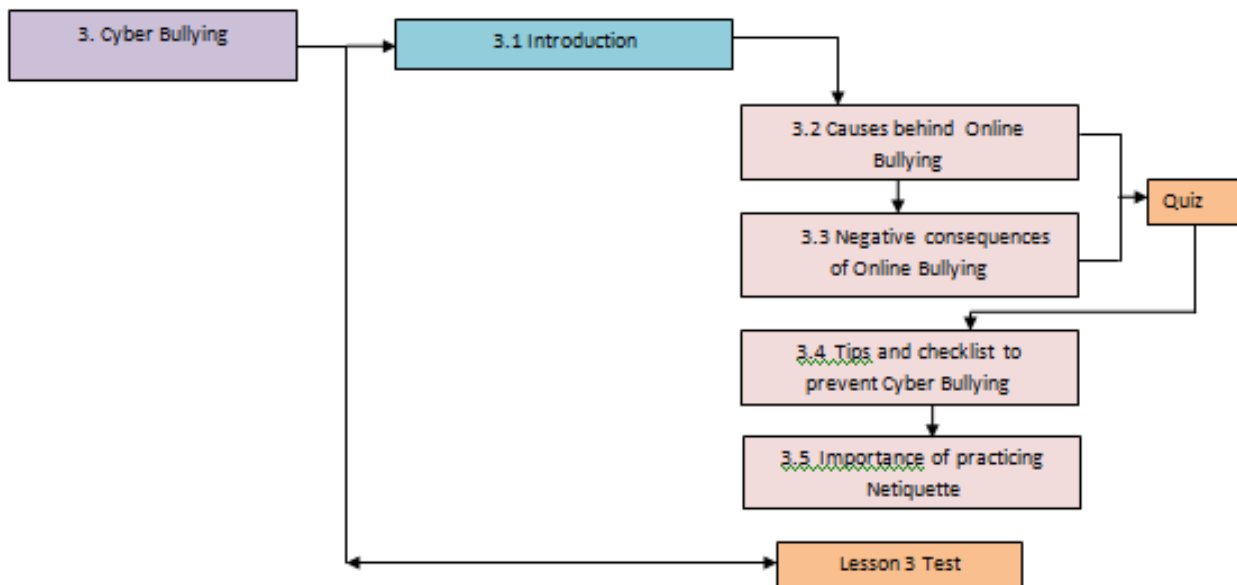| Type of Incident	Year 2008
Phishing	5
Abuse/Privacy	3
Scams	5
Malware	11
Defacements	14
Hate/Threat Mail	6
Unauthorized Access	5
Total	**49**

APPENDIX G

Detail Course Map

Lesson 2 – Online Reputation
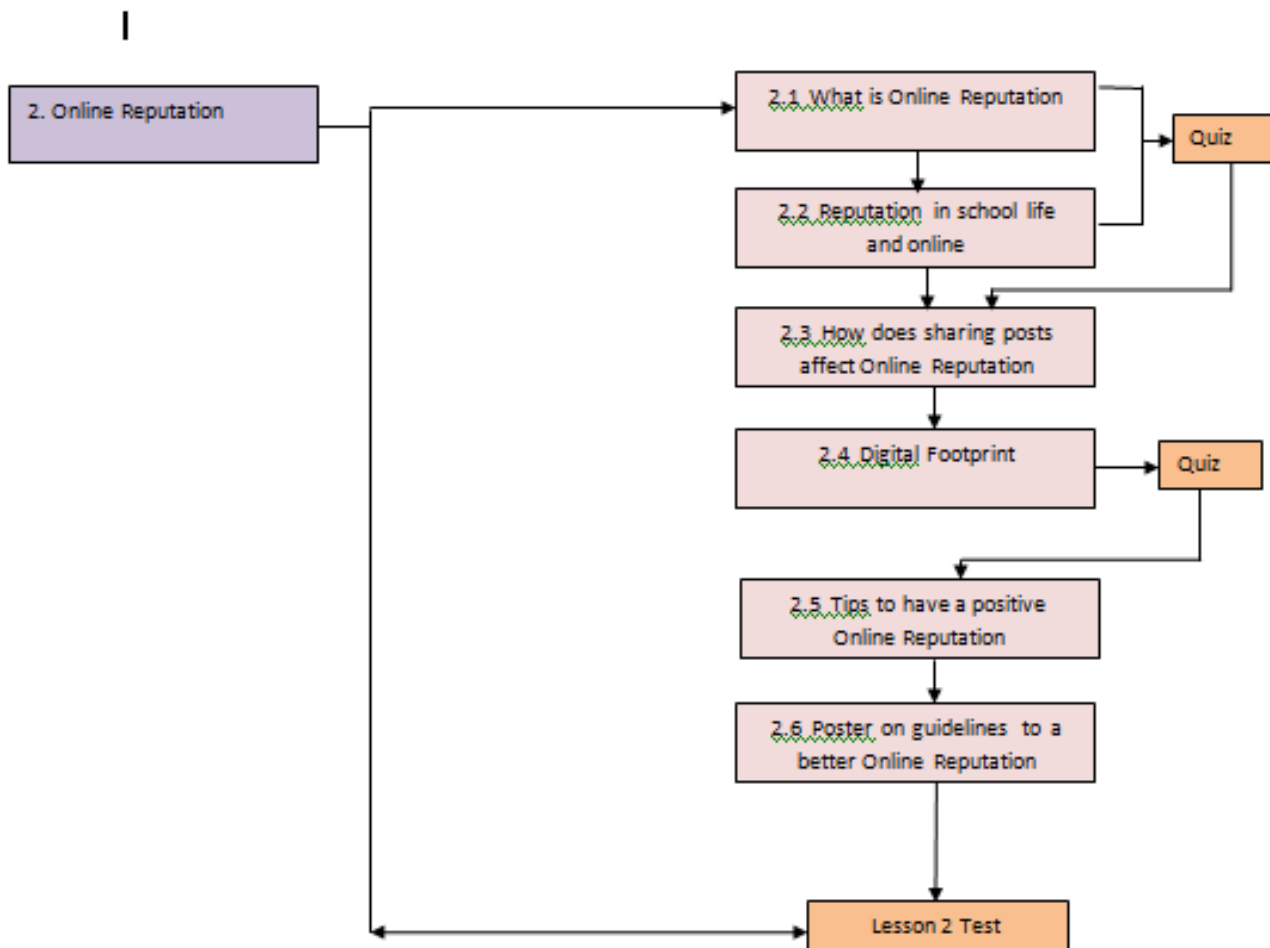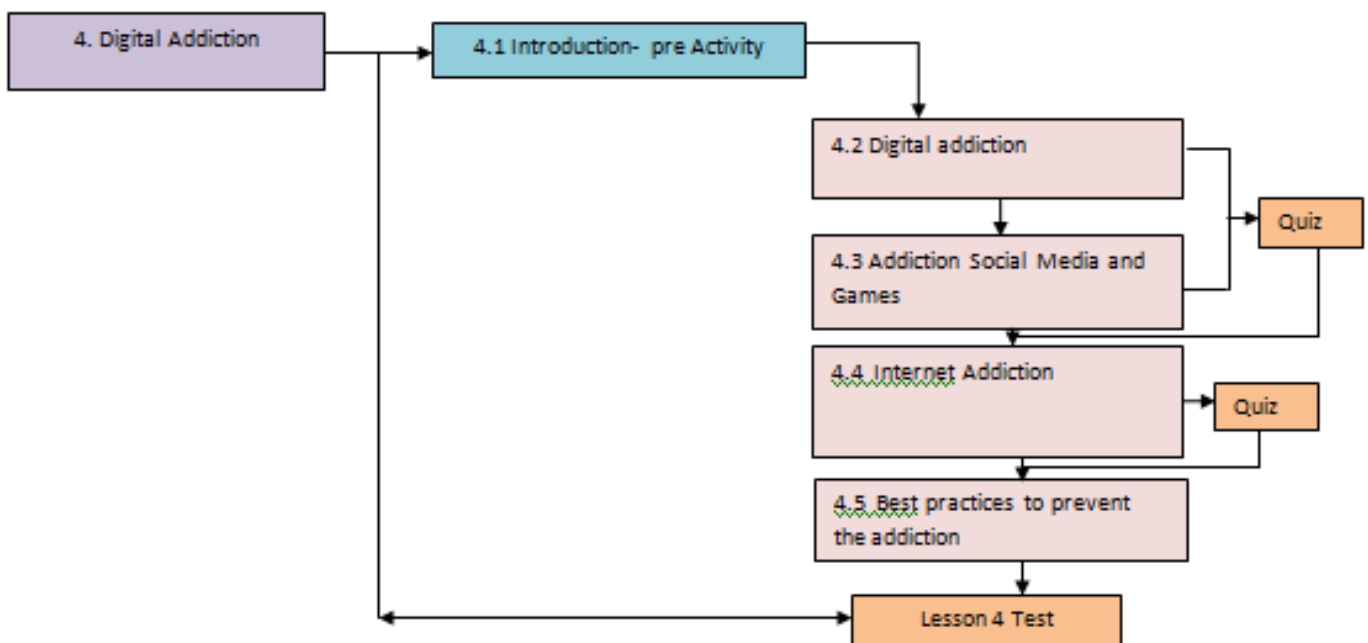
APPENDIX G

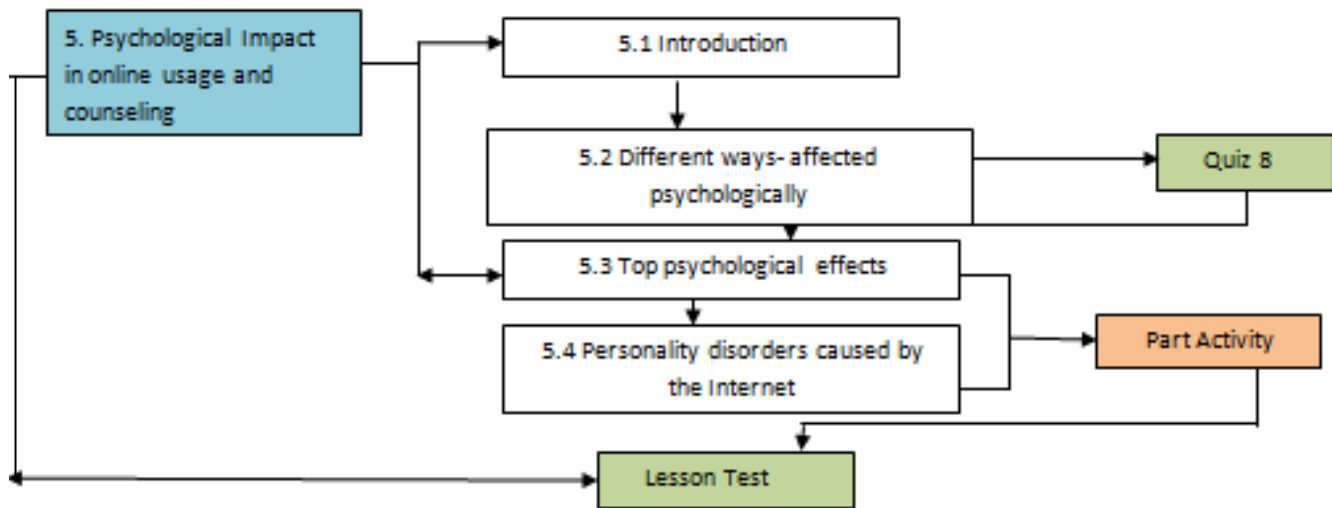## Lesson 3- Cyber Bullying

Lesson 4- Digital Addiction

APPENDIX G

Lesson 5 - Psychological impact in online usage

Lesson 6- Internet Safety and reporting crime