Cyber Safety Education in Developing Countries

Rossouw VON SOLMS
Nelson Mandela Metropolitan University
P.O Box 77000, NMMU, Port Elizabeth, 6031, South Africa

and

Suné VON SOLMS
Council for Scientific and Industrial Research,
Meiring Naude Road, Pretoria, 0184, South Africa
North West University,
Hoffman Street, Potchefstroom, 2520, South Africa

ABSTRACT

Cyber safety has become critical in today's world. Young children specifically need to be educated to operate in a safe manner in cyberspace and to protect themselves in the process. Unfortunately, African and developing countries do not necessarily possess the required resources to run extensive educational programmes for children. Using open educational resources, a cyber-safety curriculum has been developed. This curriculum will empower teachers in junior or primary schools to educate their learners about cyber safety. Once all the tests have been completed, the curriculum will be made available to primary schools in countries where governments or education departments do not provide such educational material.

Keywords: Cyber safety, cyber security, cyber education, cyber awareness

1. INTRODUCTION

The objective of cyber-safety education is to educate the users of technology on the potential risks that are faced when using Internet communication tools, such as the social media, chat rooms, online gaming, email and instant messaging [1],[2] When users are educated about these risks, the users' vulnerability to malware attacks, cyber-bullying and identity theft can be considerably reduced [3]. Young children are very vulnerable to becoming victims of cyber security attacks, as they are curious and enthusiastic about exploring the online world, but may not be aware of all the risks associated with the usage of Internet communication tools [4].

Children are taught from a young age to stay physically safe in their school, house and community. Teachers, parents and guardians teach them not to talk to strangers, how to cross a road safely etc. Just as they are taught to stay safe in the real world, they should be taught how to stay safe in the online world as well.

In developed countries, an exhaustive range of Cyber Safety Initiatives are active in the plight to keep kids safe online. The European Union's initiatives include ins@fe [5], Safer Social Networking Principles for the EU [6] and European Framework for Safer Mobile Use by Younger Teenagers and Children [7]. As early as 2009, education on Online Safety was included in school curricula in 24 European countries [8]. Similar cyber-safety initiatives in the USA are supported by the Department of Homeland Security [9], National Cyber Security Alliance [10] and the Multi-State Information Sharing and Analysis Center [11].

Cyber safety education in developing African countries, however, faces various challenges, which includes the lack of comprehensive cyber safety initiatives, limited governmental support [12], as well as inadequate cyber safety curricula or extramural activities [13], limited budgets, resources and knowledge by teachers. Due to the lack of education initiatives and resources in this regard, school children are becoming increasingly more vulnerable to cyber-safety attacks.

The objective of this paper is to show why it is so critical that modern-day school children or learners are educated about the risks associated, while being active in cyberspace, what factors are hampering such education, and lastly to propose a curriculum that can be used by teachers in junior or primary schools, specifically in developing and/or African countries to empower such education.

The outline of this paper is as follows: The main reasons for cyber safety education will be discussed in Section 2, where the difficulties and challenges of such education will be presented in Section 3. In Section 4, open educational resources and the advantages thereof will be mentioned. Sections 5 and 6 include the broad methodology followed and the proposed curriculum for cyber safety education for primary schools, respectively. Lastly, the paper will be concluded in Section 7.

2. MOTIVATION FOR CYBER-SAFETY EDUCATION

The need for comprehensive cyber-safety education stems from the rapid growth in Internet demand across Africa in the last decade. In a forecast by TeleGeography [14], Africa's demand for bandwidth has a projected growth of 51% per annum, outpacing all other markets worldwide. Researchers predict that internet use on mobile phones in Africa will increase at double the rate of that in the rest of the world in the next five years, reaching 1 billion mobile subscribers in Africa by [15] and approximately 1 billion subscribers in sub-Sahara Africa by 2019 [16].

The drop in costs of mobile handsets and mobile data makes cellular phones a very attractive method to stay connected in rural African areas with limited infrastructure. The use of mobile applications to assist in banking [17], farming [18] and health [19] is increasing in popularity; as it greatly improves the welfare of Africans [20]. The downside to the rapid advance in

internet usage in Africa is that legislation relating to cyber crime [21], computer literacy and education [22] has failed to maintain the desired pace, and to keep up. This delay has caused all users of the Internet, including children, to be vulnerable to cyber attacks and threats.

Cyber threats and attacks can come in many shapes and forms; but they can be divided into four [22], [23].

1) Technology-based threats, which can include the spreading of malware, spyware and hacking.
2) Content-related risks, where a person is subjected to harmful or offensive content, or where a person is influenced to produce and distribute such content.
3) Threat of harassment, which includes any form of unwanted contact or attention, such as cyber bullying.
4) Exposure-related threats that include any situation, where personal or sensitive information is exposed.

These threats and attacks can come in many forms – where users are not always aware that they are being attacked. Therefore, it is essential to educate and empower users, especially children, on the safe and responsible use of online resources and platforms to establish a cyber-safety culture [4],[12]. The establishment of a cyber-safety culture amongst the youth would ensure that they become responsible digital citizens and contribute to the future of cyber security across Africa.

3. CHALLENGES OF CYBER-SAFETY EDUCATION

The various cyber safety-education role-players have been widely documented [2],[12],[22],[23],[24]. These can be divided into six sectors, which include government, law enforcement, parents/guardians, schools, teachers and peers. These role players all have a different role to play in the establishment of a cyber-safety culture. These roles range from the development and enforcement of cyber-safety legislation, to the provision of funding for the creation of cyber-safety initiatives and curricula, to support for the safe and responsible online use.

There are, however, limited initiatives to educate children on cyber safety across Africa. Only a handful of African governments currently have active cyber-safety education and awareness initiatives. These include Tunisia [25], Rwanda [26], Ghana [27], Cameroon [28], Egypt [29], Kenya [30], Mauritius [31] and Rwanda [32].

At the African Internet Governance Forum (AFIGF), held in September 2013, information and technology stakeholders discussed how cyber-safety policies could be implemented by the governments of African countries, in order to combat cyber crime in Africa. The participants stated that government must adopt strategies in which cyber-safety curricula/syllabi are introduced in schools, and where teachers are trained in cyber safety [33].

The introduction of cyber-safety curricula in schools, however, is not a simple task, because of the lack of funding and the scarcity of resources available at the schools, as well as the lack of experience and knowledge by teachers on cyber-safety threats and the corresponding safety measures [2],[4],[23]. Nevertheless, cyber-safety awareness in schools cannot lie dormant until effective government initiatives are implemented, since children, teachers and parents are regularly confronted with children falling victim to cyber attacks and threats. Children must be equipped with the knowledge to use the Internet safely and responsibly by any and every means possible.

4. OPEN EDUCATIONAL RESOURCES

The use of Open Educational Resources (OER) can support teachers and schools in educating children on cyber safety. OER can be defines as: "Teaching, learning, and research resources that reside in the public domain, or have been released under an intellectual property licence that permits their free use and re-purposing by others. Open educational resources include full courses, course materials, modules, textbooks, streaming videos, tests, software, and any other tools, materials, or techniques used to support access to knowledge" [34].

The advantages for teachers and schools in utilizing OER include the following [35], [36]:

1) The material is developed for educational purposes; therefore, the schools are not required to develop a curriculum themselves.
2) All resources are free and readily available, so learning material can be accessed without the need for a user account.
3) OER material is kept up-to-date. This ensures that children can learn about the latest cyber-safety issues.
4) Resources are developed for a range of subjects and age groups.

In von Solms & von Solms [4], a baseline cyber-safety curriculum was presented as the first step in the development of an open educational resource for cyber-security education in Africa. The baseline curriculum was built on a selection of publicly available videos from YouTube.com and ThinkYouKnow.co.uk that can be used in a classroom environment to educate children on various cyber-safety issues. Three "curriculum tables" for age groups 7-9 years, 10-12 and 13+, were created that contained the URL to the video and the cyber safety topic.

This paper discusses the full curriculum, based on the work previously presented in von Solms & von Solms [4], where the online videos are combined with lesson plans, activities and discussion topics to support teachers in conveying each cyber-safety message.

5. METHODOLOGY

The goal of this paper, as set out earlier, is to describe the process followed to develop and test a curriculum to teach cyber safety to junior or primary school learners, specifically in developing countries, where the necessary resources and support are not always readily available.

The following assumptions were taken into account during the development of the curriculum:

- Governments and national departments of education would not necessarily see cyber-safety education as a national priority.

- School curricula are fairly congested; and little additional time might be available to offer cyber-safety educational lessons to learners during formal school times.
- The management of schools, and the teachers at schools, might not necessarily be enthusiastic about, or capable of offering cyber safety to learners.
- Teachers should be empowered and educated on cyber safety, whilst preparing individual lessons.
- The lessons should be fun and enjoyable.
- Proper lesson plans should be made available to teachers to ensure minimal preparation and effort.

The following methodological process was followed to develop and test the envisaged curriculum.

Firstly, applicable resources should be identified to be used as presentation material to convey the educational principles of cyber safety to the learners. To ensure that all lessons will be enjoyable and fun to the learners, it was decided that only cartoon videos with an applicable educational message would be used. Thus, the core presentation resource for each lesson was envisaged to be a cartoon video from the online video-sharing website, YouTube. A proper content analysis of the videos should be conducted to ensure: Applicability, as far as cyber-safety education is concerned, the core cyber-safety message from the video and the typical age grouping to which the video might be applicable. This exercise should result in a series of very applicable cartoon videos that could be used to convey education cyber-safety principles and messages to learners.

Secondly, these resources must be packaged in lesson plans for teachers, in order to enable and empower them to easily prepare, present and access such a lesson.

Thirdly, some alpha-testing needs to be run to ensure that everything is working well in a classroom situation; and this should be followed by some beta-testing in a number of schools.

Finally, after feedback from teachers, where some beta-tests were run, some final amendments should take place.

6. A CURRICULUM FOR TEACHING CYBER-SAFETY IN JUNIOR OR PRIMARY SCHOOL

Having worked through hundreds of cartoon videos, readily available on YouTube, 47 very applicable videos were identified. An experienced cyber safety/security researcher and a junior/primary school teacher with many years of experience identified the core cyber-safety messages, as well as the most applicable age grouping for each of these 47 videos.

Broadly, the educational messages from these 47 videos could be classified into the following broad categories: Oversharing of personal and private information, cyber bullying, and being nasty to others, strong password selection, identity theft, online 'friends' might not always be those who they pretend to be, online game addiction, your online profile stays with you forever, and can count against you years later, sexting and information spreads very fast online. Further, these videos were classified into three age groupings, namely: 6 to 9 years, 10 – 12 years and 13+ years. Thus, 47 suitable cartoon videos from YouTube and ThinkYouKnow.co.uk, with suitable educational cyber-safety messages were identified, classified and grouped.

As mentioned earlier, the teachers are not necessarily knowledgeable enough to offer cyber-safety lessons, or to facilitate a discussion on the specific topic. For this reason, comprehensive lesson-plans to assist teachers to offer these lessons are definite prerequisites. The development of extensive and comprehensive lesson-plans was done by 4th year students in an Information Security IV course at a university in Port Elizabeth, South Africa. Guidelines for good lesson plans [36] were given to seven two-person student teams as a class assignment. The best set of lesson plans from these seven groups was chosen. Each of the lesson-plans consists of the following:

- An Overview of about half an A4 page, providing background information on the lesson, what the core educational aspects in the lesson are, and what the learners should learn from the lesson. This Overview assists the teacher with preparation for the lesson and discussion afterwards. An overview of a typical lesson appears below.

Overview:
At this young age, children are very vulnerable, as they trust others easily. They are also very naïve. Most children are on Facebook or other social media platforms. A person can be found on these platforms by simply searching their names. Your own information stays private until you confirm that person's friendship request. By confirming the friendship request, you confirm that you know that person, and that you trust that person to view your personal information and daily activities. This lesson, the first of a new cartoon series, addresses the issue of friendship requests; and it emphasizes children's sometimes naïve attitude towards accepting friendship requests on the social media. The main message of the video explains that by confirming a Facebook friend, you invite them into your life. It is important that children know what consequences accepting a stranger on social media could have.

- Some Learning Objectives are set for every lesson – to ensure that the lesson is offered with a specific goal in mind. An example appears below.

Learning Objectives:	Primary: Comprehend the dangers of accepting strangers on social media as friend.
	Secondary: 1. Know why it is important to only accept people you know as friends. 2. Understand that you invite people into your life when you accept them as friends on social media.

- The Materials to be used in the lesson are merely a hyperlink to the relevant YouTube video to be shown in the lesson. The teacher can merely *click* on the hyperlink to download and show the video. See example below.

Materials:	Funmoods' Online Safety Kit - Little Red Riding Mood: Chapter 1.

	https://www.youtube.com/watch?v=KGr_KFiCX4s

- The Procedure to offer a typical lesson is spelt out to the teacher, thus what should follow, and in which order. Example below.

Procedure:	1. Overview of social media and friendship requests. 2. Watch the video. 3. Reflect on the video with a class discussion. 4. Explain the concepts of the main lesson. 5. Do class assessment to measure the level of understanding and insight.

- A number (between four and six) of Discussion Questions were prepared for every lesson. The teacher should ideally discuss these questions after the lesson, to ensure that the learners understood the content and the educational material. A typical example of some discussion questions is shown below.

Discussion Questions:	1. Which social media platforms are available? 2. Who should you not accept as a friend? 3. What might the consequences be of accepting a stranger? 4. What happened after Little Red Riding Hood had accepted the friendship request? 5. What did you notice about the profile photo the wolf had on his profile? 6. How easy is it for someone to make a fake Facebook profile?

- A lesson Assessment page is also prepared for each lesson. The assessment evaluates whether the learner has understood the lesson and the educational message. The format of these assessments includes small crossword puzzles, short comprehension tests, word searches, etc. The idea is that each learner should ideally receive such an assessment page to complete individually.

Each lesson, consisting of the lesson plan for the teacher on one A4-page and the assessment exercise on another A4-page, is stored in a pdf document.

Finally, a total of 33 such lesson plans were prepared, and then divided into the three age groupings. An index document was also created, in which all the lessons with their main topic focus areas (e.g. cyber bullying, oversharing, etc.) are listed in the three age groupings. Hyperlinks to the respective lessons were created – to make it easy for the teachers to get to the respective lessons. The Cyber-Safety Curriculum was saved on a CD; and it consisted of the Index document together with all the lessons.

Following the development of the material, the Cyber-Safety Curriculum was provided to one primary school to run some initial or alpha-tests. The teacher responsible for IT education at the school did offer a number of the lessons to a number of different age groups. The teacher reported that the lessons were easy to prepare; the learners thoroughly enjoyed the videos; and some useful educational discussions were based on the discussion questions provided. The teacher remarked that a memorandum to the assessment page would be appreciated. Based on this remark, a memorandum page for each of the lessons was prepared; and this was then added to each lesson.

Subsequently, a number of primary schools in the region of the university in Port Elizabeth were invited to a Cyber-Safety Workshop, where the curriculum would be discussed and distributed. Twenty-eight teachers from twenty-one local primary schools attended the workshop. The motivation for, and the background to the cyber-safety curriculum were presented to the teachers attending the Workshop. The teacher from the school that participated in the initial alpha-testing also shared his experience and enthusiasm with those attending. All the teachers were invited to participate in a second and final round of testing (beta-testing). Everybody accepted the invitation, and undertook to participate in running and testing the curriculum. A complete curriculum was therefore provided on CD to each of them. The attendees were asked to complete a questionnaire in six weeks' time to report any errors, improvements, shortcomings, etc., but all felt it should rather be done in the New Year; as all the schools were busy with end-of-year examinations. Thus, official feedback from the beta-testing exercise will only be available at a later stage.

The initial feedback received was very positive. One teacher reported that she ran a lesson the following day with minimal preparation, but she felt very confident in offering the lesson and discussing the questions afterwards. She mentioned that the learners "LOVED" it – specifically as they could associate with well-known characters like, Little Red Riding Hood. Another teacher reported that the lesson was really informative and exciting and that the video lesson was 'a real hit'.

Although the cyber-safety curriculum will only be finalised and extensively made available at a later stage, it can definitely be classified as filling a huge gap in the educational programme in junior or primary schools – and that it will prove to be very helpful to schools and teachers that want to educate their learners on the risks and controls relating to cyberspace.

Developed countries are providing millions of pounds, euros, or dollars to offer cyber-safety programmes in schools, in media, or over television. Unfortunately, this is not the case in most developing countries; but children in these countries are as exposed to the risks in cyberspace as are the children in developed countries. This cyber-safety curriculum, once finalised and made available to everybody, should at least assist in this regard.

7. CONCLUSION

Cyberspace is used by more and more people daily, especially children. Most children use services like social networking, electronic communication etc.; and they do so on a daily basis. Along with all the advantages offered by these cyber services, numerous risks appeared. For this reason, our children need to be educated to protect themselves, whilst learning to be active in cyberspace.

In many cases, governments lead such educational programmes; but in most African and other developing countries this is not necessarily the case – even though these children are just as

exposed to similar risks. Therefore, it is important that suitable curricula should be made available, free of charge preferably, to ensure that children in these countries can also become IT-educated. For this reason, a cyber-safety curriculum that makes use of open educational resources was developed. The curriculum is based on educational cartoon videos with cyber-safety messages. These videos have been packaged in a curriculum, along with detailed lesson plans. These lesson plans assist teachers to learn with the learners; and they are easy to prepare and offer. Each lesson plan is also accompanied by an assessment exercise for the learners to test whether they have understood the material.

The idea is, once the curriculum is fully tested, that it should be made freely available to teachers in developing countries, where such government-driven programmes are not yet available.

9. REFERENCES

[1] Microsoft, "Online predators: Help minimize the risk",. [Online] Available at: "http://www.microsoft.com/security/family-safety/predators.aspx", 2014. Accessed on [20 November 2014].

[2] D. Miles, "Youth protection: Digital citizenship - Principles and new resources", **Second Worldwide Cybersecurity Summit (WCS)**., 2011.

[3] I.Z. Dlamini, B Taute, J Radebe, "Framework for an African Policy Towards Creating Cyber Security Awareness", [Online] Available at: "http://books.google.co.za/books?id=SrivoAEACAAJ", 2011. Accessed on [20 November 2014].

[4] S. von Solms and R. von Solms, "Towards Cyber Safety Education in Primary Schools in Africa", **Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)**, pp.185-97, 2014.

[5] Ins@fe, [Online] Available at: "http://www.saferinternet.org/home", 2014. Accessed on [13 February 2015]

[6] N. Fabiano et.al, "Safer Social Networking Principles for the EU", [Online] Available at: "https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf", 2009. Accessed on [13 February 2015].

[7] GSMA, "European Framework for Safer Mobile Use by Younger Teenagers and Children", [Online] Available at: "http://www.gsma.com/gsmaeurope/safer-mobile-use/european-framework/", 2009. Accessed on [13 February 2015].

[8] EACEA, "Summary Report: Education on Online Safety in Schools in Europe", [Online] Available at: "http://eacea.ec.europa.eu/education/eurydice/documents/thematic_reports/121EN.pdf", 2010. Accessed on [13 February 2015].

[9] Department of Homeland Security, "National Cyber Security Awareness Month 2014", [Online] Available at: "http://www.dhs.gov/national-cyber-security-awareness-month-2014", 2014. Accessed on [13 February 2015].

[10] National Cyber Security Alliance, "Stay Safe Online", [Online] Available at: "https://www.staysafeonline.org/", 2014. Accessed on [13 February 2015].

[11] Multi-State Information Sharing and Analysis Centre, [Online] Available at: "http://msisac.cisecurity.org/", 2014. Accessed on [13 February 2015].

[12] N. Kortjan and R. von Solms, "Cyber Security Education in Developing Countries: A South African Perspective", **Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering**, pp.289-97, 2013.

[13] E. Kritzinger, "Cyber Awareness Implementation Plan (CAIP) for schools", **Presentation for Southern African Cyber Security Awareness Workshop (SACSAW)**, 2011.

[14] TeleGeography, "Africa's international bandwidth growth to lead the world", TeleGeography: Global Bandwidth Forecast Service. [Online] Available at: "https://www.telegeography.com/products/commsupdate/articles/2013/10/31/africas-international-bandwidth-growth-to-lead-the-world/", 2013. Accessed on [22 November 2013].

[15] M. Reed, "Press release: Africa mobile subscriptions count to cross 750 million mark in fourth quarter of 2012", **Informa Telecoms & Media**, 2012.

[16] D. Smith, "Internet use on mobile phones in Africa predicted to increase 20-fold", The Guardian. [Online] Available at: "http://www.theguardian.com/world/2014/jun/05/internet-use-mobile-phones-africa-predicted-increase-20-fold", 2014. Accessed on [12 November 2013].

[17] Migrant, " M-PESA International Money Transfer Service", Safaricom. available [Online] Available at: http://www.ilo.org/dyn/migpractice/migmain.showPractice?p_lang=en\&p_practice_id=70, 2013. Accessed on [12 November 2013].

[18] Safaricom, "iCow", [Online] Available at: "http://www.safaricom.co.ke/personal/value-added-services/social-innovation/icow", 2012. Accessed on [12 November 2013].

[19] M. Mars and L. Erasmus, "Telemedicine can lower health care costs in Africa", **Innovate**, pp.32-33, 2012.

[20] PWC, "Telecoms in Africa: innovating and inspiring". Communications Review, 2012.

[21] M. Grobler and Z. Dlamini, "Global Cyber Trends a South African Reality", **Conference Proceedings of IST-Africa,** 2012.

[22] M. de Lange and R. von Solms, "An e-Safety Educational Framework in South Africa", **Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC)**, 2012.

[23] S. Atkinson, S. Furnell and A. Phippen, "Securing the next generation: enhancing e-safety awareness among young people", **Computer Fraud & Security**, pp.13-19, Available at: "http://www.sciencedirect.com/science/article/pii/S1361372309700880", 2009. Accessed on [12 November 2013].

[24] Becta, "AUPs in context: Establishing safe and responsible online behaviors", [Online] Available at: http://education.qld.gov.au/studentservices/behaviour/qsaav/docs/establishing-safe-responsible-online-behaviours.pdf, 2009. Accessed on [10 November 2013].

[25] K. Cole et al., "Cybersecurity in Africa: An Assessment', [Online] Available at: http://s3.amazonaws.com/zanran_storage/www.cistp.gatech.edu/ContentPages/43945844.pdf, 2008. Accessed on [22 November 2013].

[26] F. Kanyesigye, New Times. [Online] Available at: http://www.newtimes.co.rw/news/index.php?a=66437\&i=15343, 2013. Accessed on [22 November 2013].

[27] E. Antwi-bekoe and S.G. Nimako, "Computer Security Awareness and Vulnerabilities: An Exploratory Study for Two Public Higher Institutions in Ghana", **Journal of Science and Technology**, pp.358-75, 2021.

[28] International Telecommunication Union, "Cyberwellness Profile: Camaroon", [Online] Available at: "http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Cameroon.pdf", 2014. Accessed on [28 November 2014].
[29] International Telecommunication Union, "Cyberwellness Profile: Egypt", [Online] Available at: "http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Egypt.pdf", 2014. Accessed on [28 November 2014]
[30] International Telecommunication Union, "Cyberwellness Profile: Kenya", [Online] Available at: "http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Kenya.pdf", 2014. Accessed on [28 November 2014].
[31] International Telecommunication Union, "Cyberwellness Profile: Mauritius", [Online] Available at: "http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Mauritius.pdf", 2014. Accessed on [28 November 2014].
[32] International Telecommunication Union, "Cyberwellness Profile: Rwanda", [Online] Available at: "http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Rwanda.pdf", 2014. Accessed on [28 November 2014].
[33] N. Sato, "ICT stakeholders discuss emerging issues on African cyber security", [Online] Available at: http://www.humanipo.com/news/32773/ict-stakeholders-discuss-emerging-issues-on-cyber-security, 2013. Accessed on [21 November 2013]..
[34] The William and Flora Hewlett Foundation, "Open Educational Resources", [Online] Available at: "http://www.hewlett.org/programs/education/open-educational-resources", 2014. Accessed on [22 November 2013]..
[35] OER Africa, " Understanding OER", [Online] Available at: "http://www.oerafrica.org/understandingoer/UnderstandingOER/tabid/56/Default.aspx", 2013. Accessed on [20 November 2013].
[35] Jisc.ac.uk, "A guide to open educational resources" [Online] Available at: "http://www.jisc.ac.uk/publications/programmerelated/2013/Openeducationalresources.aspx", 2012. Accessed on [20 November 2013].
[36] Education Oasis, “Help with lesson planning”, [Online] Available at: http://www.educationoasis.com/curriculum/LP/lesson_plans.htm, 2011. Accessed on [19 August 2014].