Towards Cyber Safety Education in Primary Schools in Africa

S. von Solms[1,2] and R. von Solms[3]

[1]Council for Scientific and Industrial Research, Pretoria, South Africa
[2]North West University, Potchefstroom, South Africa
[3]Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
e-mail: svsolms@csir.co.za; rossouw@nmmu.ac.za

Abstract

Cyber safety has become critically important to all who are active in cyber space. In most African countries no coordinated activities in this regard are taking place, even though many children are already active on cyber space. This paper presents an introductory, but usable, guide to empower primary school teachers, specifically in Africa, to impart the basic principles of cyber safety to their learners. A set of very usable, self-explanatory, publicly available online video cartoons were identified for use as resources by teachers in discussing and stimulate cyber safety principles to primary school learners.

Keywords

Cyber safety, cyber security, cyber awareness, cyber education.

1. Introduction

Internet usage has increased significantly across Africa in the past few years through the increase in bandwidth, wireless technologies and infrastructure. In fact, Africa has the fastest growing market in terms of information technology growth (TeleGeography, 2013). This increase in Internet usage throughout Africa offers a wide range of advantages, but also increases users' vulnerability to malware infection, cyber-bullying, identity theft and cyber terrorism (Dlamini, Taute, & Radebe, 2011). Africa mainly consists of developing countries which are characterised by limited knowledge, expertise and understanding regarding cyber safety (Dlamini, Taute, & Radebe, 2011), (e4Africa, 2011). Young children especially are at risk as they may not know the dangers associated with cyber space.

Many developing countries in Africa do not currently have comprehensive cyber safety initiatives in place (Kortjan & von Solms, 2013); this is exacerbated by the fact that schools have no available curricula or extramural for cyber safety education (Kritzinger, 2011). Teachers' limited knowledge regarding cyber safety, together with limited budgets and resources make the education of children on cyber safety issues extremely challenging. School children in Africa are becoming ever more active in cyber space and few schools are offering any cyber safety education to teach these children safe practices whilst online. Along with this, almost all teachers are ill equipped to understand and offer assistance in and hardly any resources are

available to schools and teachers in this regard. Further, hardly any African governments are providing any governmental support in attempting to raise the levels of cyber safety amongst school children. Thus, cyber safety among the youth in most African countries is becoming a growing problem.

The objective of this paper is an attempt to empower African school teachers to educate children on cyber safety by learning along with their learners and by identifying freely available resources on the Internet. This paper aims to provide a guide or basic syllabus to empower teachers in primary schools to teach children to protect themselves when exploring the online world by means of safe and responsible online behaviour and in the process teachers will also educate themselves in this regard.

The next section describes the modern cyber space, its growth, the services it offers as well as the risks associated with it. Section 3 discusses education towards a cyber secure culture and Section 4 will look at the problem of cyber safety education in schools. Section 5 discusses the methodology followed to form a basic syllabus, which is proposed in Section 6. Section 7 will conclude this paper.

2. Modern Cyber Space

It is projected that Africa's demand for Internet access will grow by an average of 51% every year until 2019 (TeleGeography, 2013) and that there will be approximately 1 billion mobile cellular subscribers in Africa by 2015 (Reed, 2012).

Access to the Internet through mobile phones in Africa is becoming more widely available, consequently impacting on the lifestyle and well-being of communities (PWC, 2012). This includes the improvement of banking, healthcare, farming and many other practices. M-Pesa, the international money transfer service launched by Safaricom in Kenya in 2007, has enabled Kenyans to transfer and receive funds and conduct other basic banking transactions using their mobile phones (Safaricom, Relax, you've got M-Pesa, 2012). By March 2012, the number of active M-Pesa users was approximately 14,6 million (Migrant, 2013). Farmers are utilising their mobile phones to get daily updates on the weather, the directions of locust swarms and commodity prices. They also use mobile applications, like iCow by Safaricom, which enable dairy farmers to monitor their cows, receive farming advice and veterinary assistance (Safaricom, iCow, 2012). Mobile phones greatly assist healthcare in rural areas, as people can enjoy access to medical specialists and services from clinics without the need to take long journeys on foot to the nearest health care centre (Mars & Erasmus, 2012). As can be seen, the use of the Internet has greatly enhanced living standards in many respects.

The rapid growth in Internet usage also, unfortunately, makes African countries vulnerable to cyber-attacks and threats owing to high levels of computer illiteracy and ineffective or insufficient legislation (Grobler & Dlamini, 2012). All users of ICT, which includes the private and the public sectors, government, and the general public, including school children (de Lange & von Solms, 2012), are vulnerable to

these attacks and threats. Internet users may be exposed to a range of threats, including (de Lange & von Solms, 2012), (Atkinson, Furnell, & Phippen, 2009):

- Technology-focused threats, i.e. hacking, malware and spyware.
- Content-related risks, i.e. exposure to illicit or inappropriate content.
- Harassment-related threats, i.e. cyber-bullying, cyber-stalking and other forms of unwanted contact.
- Risk of exposing information, i.e. children exposing their personal information through phishing or sharing information on social networking platforms.

In many cases, people tend to think that all these potential risks can be eliminated completely by means of technology-based solutions, like blocking or filtering software to restrict what children access online. There are several technologies that can greatly assist in keeping users safe online, but the use of the Internet can never be completely safe (Atkinson, Furnell, & Phippen, 2009), (Byron, 2008). Thus users of cyber space need to be educated to develop safe and responsible online behaviour in order that they will be empowered to protect themselves while exploring the online world (Becta, 2009).

3. Education towards a Cyber Safety Culture

Children can be especially vulnerable to cyber threats as most children are curious and enthusiastic to explore new technologies and environments. In addition, they are naive and unaware of the dangers they may face. As children are educated by parents, guardians and teachers to make wise decisions when dealing with their daily life, like not talking to strangers, walk in unsafe places or to give away personal information, they should be taught how to make wise decisions online as well. This includes using a cell phone, searching the web and using social networking platforms in a safe and responsible manner (Miles, 2011).

The education of children regarding cyber safety threats is vital in order to establish a cyber secure culture (Kortjan & von Solms, 2013). It is stated that the education of children on safe Internet usage will encourage support and knowledge sharing among peers, which would instil the confidence in children to practise safe online behaviour (Atkinson, Furnell, & Phippen, 2009), (Becta, 2009). Today's youth is the guardians and teachers of the future, and teaching them to be responsible digital citizens will have a massive impact on the establishment of a cyber secure culture. Thus the establishment of a culture of cyber safety through education and empowerment is therefore a vital part of addressing the growing threats of Internet usage.

The fact that there are several role players in the cyber safety education of children is widely supported. These role players include (Kortjan & von Solms, 2013), (de Lange & von Solms, 2012), (Atkinson, Furnell, & Phippen, 2009), (Becta, 2009), (Miles, 2011):

- *Government*. Government should develop structures to adequately support cyber safety, establish and promote a cyber safety culture through support and funding toward research and education of cyber safety initiatives and encourage compliance with cyber safety standards.
- *Law enforcement*. Legislation relating to cybercrime toward children is critical to protect them against cyber-bullying, cyber-stalking, online harassment and so on.
- *Parents/guardians*. Parents or guardians have the most direct influence on children and play a vital role in cyber safety education and awareness, which includes education on safe and responsible usage, rules and assistance when using the Internet.
- *Schools.* Cyber safety strategies should be developed and implemented in schools.
- *Teachers*. Teachers should be knowledgeable in the field of cyber safety, act as advisors to children, deliver the cyber safety messages and act as observers in noticing changes in a child's behaviour.
- *Peers*. Peer mentoring is a very effective way of encouraging children to stay safe online. Encouragement, support and sharing of knowledge give children more confidence to practise safe online behaviour.

According to the Africa Child Online Protection Education and Awareness (ACOPEA) centre there is no concrete PAN-African child online protection education and awareness model in Africa (ACOPEA, 2012) and limited cyber security awareness and education initiatives in developing African countries (Kortjan & von Solms, 2013). A summary of selected African countries' cyber safety efforts toward education and awareness is shown in Table 1:

Country	**National cyber safety awareness and education**
Uganda	×
Sudan	×
Tunisia	√ (Cole, Chetty, Larosa, Rietta, Schmitt, & Goodman, 2008)
Rwanda	√ (Kanyesigye)
Egypt	×
Morocco	×
Kenya	×
Cameroon	×
Ghana	√ (Antwi-bekoe & Nimako, 2012)
Mauritius	√ (Dlamini, Taute, & Radebe, 2011)

Table 1: Cyber safety efforts by selected African countries

With the lack of comprehensive cyber safety initiatives in many African countries, the increase in Internet usage is not matched with sufficient education and awareness (Dlamini, Taute, & Radebe, 2011), (e4Africa, 2011). This greatly affects the manner and effectiveness in which the abovementioned role players can assist in creating a cyber aware culture.

During a discussion on cyber safety at the African Internet Governance Forum (AFIGF) in Nairobi in September 2013, it was stated that one of the best strategies for implementing cyber safety and combatting cybercrime in Africa is for African governments to introduce cyber safety curriculums in schools (Sato, 2013). In order to assist in cyber safety education and awareness in schools, this paper focuses on teaching cyber safety to primary school learners through resources freely available on the Internet.

4. The Problem of Cyber Safety in Schools

In addition to the lack of comprehensive cyber safety initiatives in many African countries, the education of primary school children is extremely difficult owing to a lack of expert knowledge, funding and resources. Teachers may be unaware of the threats associated with cyber space as they lack experience and knowledge themselves. Schools may also not have the available funding and resources to formulate and offer a cyber safety curriculum. In addition to limited resources, technology is constantly changing and with it comes new risks and solutions. Teachers may have trouble keeping up to date with the rapidly changing landscape of the online world, the associated cyber safety threats as well as the various methods to keep them safe (Atkinson, Furnell, & Phippen, 2009), (Miles, 2011). This presents a major obstacle for teachers as they have limited access to learning material and must keep pace with the changing technological advancements.

Even though schools and teachers are faced with the abovementioned challenges, they are often faced with scenarios where children are the victims of cyber threats. Therefore, it is vital for schools to equip children with the knowledge and skills they require in order to use the Internet safely and responsible.

One method that can assist schools and teachers with limited resources is open educational resources (OER). OER are teaching and learning materials that are freely available on the Internet. This educational material can include lectures, games, assignments, videos as well as full courses and modules. All of these educational resources are available to learners and teachers without the need to create accounts or to pay royalties or licence fees (Jisc, 2012), (OER_Africa, 2013).

The utilisation of OER by African schools and teachers can greatly assist in the acquisition of relevant, current learning material. By creating a basic cyber safety syllabus from material freely available online, teachers may be empowered to educate children on using cyber space safely. The advantages of using freely available educational material include the following:

- *Material is free.* No budget is needed by schools to access this material with the exception of data fees.
- *Material can be easily accessed.* By using videos posted on YouTube and other open platforms, teachers do not have to create accounts to view or use the material.

- *Material is developed for educational reasons*. There is no need for schools to develop their own curriculum.
- *Material is up to date*. The curriculum can be updated regularly to keep children aware if the latest cyber threats and solutions.
- *Material covers a range of subjects*. The wide variety of videos available enables teachers to educate children on a wide range of current subjects.
- *Material covers age ranges*. The available videos are designed for children of various ages.

In the following 2 sections, a methodology and basic cyber safety syllabus for primary school children are presented. This syllabus is assembled from publicly available videos on YouTube and other open platforms. This syllabus can form a baseline for the future development of a complete curriculum that can be added to dedicated OER websites. In this manner, more schools can obtain easy access to a much-needed, comprehensive cyber safety education curriculum.

5. Methodology

The objective of this paper is to identify a set of effective, self-explanatory, publicly available online resources that can be used by teachers in a class situation to spread the cyber safety message to their learners. It is also assumed that these teachers are not necessarily very knowledgeable in the field of cyber safety. For this reason the material proposed also needs to educate the teachers along with the learners. Therefore, it was decided to choose a set of online videos, all readily and publicly available, to form the core of the educational resources to be used in this proposed syllabus for cyber safety for primary school learners.

On 15 November 2013 the online video-sharing website, YouTube, was searched for various cyber safety related videos. On searching the word 'e-Safety', 141 million possibilities were identified. A search for the phrase 'e-Safety for children' produced 11 million videos and the phrase 'e-Safety for children cartoon' indicated that more than 1,8 million possible cartoon videos exist. Similar searches for phrases with 'cyber safety' and 'Internet safety' revealed similar high numbers of possible videos. See Table 2 for details.

	Safety	**For children**	**Cartoons**
e-	141 m	11 m	1,8 m
Cyber	2,1 m	305 k	285 k
Internet	19 m	2 m	244 k

Table 2: YouTube searches (15 November 2013)

As the target audience for this proposed syllabus for cyber safety is restricted to primary school children, aged 7 to 13, it was decided that cartoons should be utilised as far as possible as primary school learners are very attracted to cartoons. With this in mind, 47 possible videos were initially identified. It was also decided to use the knowledge and experience of a primary school teacher with 25 years of experience to

conduct a content analysis to assist in analysing and classifying the videos. This teacher helped to analyse the contents of respective videos for suitability of use, which videos would be most suitable for which ages and which videos would have the most impact in stimulating a subsequent cyber safety discussion. At a later stage, the teacher was again used as an expert to assure that the proposed 'syllabus' was indeed usable in a typical African primary school, where Internet access was available.

The proposed methodology should ensure that a set of publicly available, online cartoon-based videos, with a clear message aimed at specific ages, forms a basic primary school syllabus that can be used in a class situation. It must be noted that the objective is not to establish a detailed syllabus with extensive lesson plans, workbooks, discussion topics, and so forth. The objective to develop a detailed syllabus is seen as future work.

6. The Video-based Syllabus for Cyber Safety for Primary School Learners

Having determined that primarily cartoon-based videos with a clear cyber safety message would be used, it was decided to analyse and categorise the 47 videos initially identified. It should again be noted that all of these videos are readily available on YouTube. Further, whilst analysing these videos, the Internet browsers, Google Chrome and Internet Explorer, did identify and suggest other possible sites for finding cyber safety related resources. One such suggestion subsequently identified a series of very popular cyber safety videos, that of Hector's World (Think_U_Know, 2008). These videos were thus also used.

All of these initially identified videos were watched, analysed and categorised with the aid of the experienced teacher. It was decided that the learners should be divided into three groups according to age, that is, 7 to 9 years of age, 10 to 12 years of age and 13 years and older. According to the experienced teacher, these are the age groups in which learners in general perform certain functions and activities online, for example, from 10 years and older, social networking and instant messaging become widely used.

The videos were categorised according to the age groups previously determined. In many cases a specific cyber safety topic is advocated by more than one video, like the message; 'Do not share your personal details.' In such cases, the videos were classified according to the most suitable age group. Most of the videos do reflect more than one cyber safety topic, but only the main topics were recorded. In Table 3, a list of cyber safety topics, the number of videos that portrayed those messages and the age groups for which such a cyber safety message is ideally suited, are reflected.

Safety topic	Number of videos	Applicable to age groups
Do not share personal information	11	7–13+
Be careful what you post online	6	10–13+
Do not be nasty to others online	1	7–13+
Choose a secure, strong password	1	10–13+
Online people are not always who you think	3	7–13+
If you feel uncomfortable, tell a responsible adult	8	7–13+
Games can be addictive	1	10–13+
Information posted online never disappears	5	10–13+
Be careful who you accept as friends	2	10–13+
A bad online profile can count against you	2	10–13+
Use privacy settings, e.g. with Facebook	3	10–13+
Cyber bullying	5	7–13+
Sexting	1	10–13+
Information spreads very fast online	1	10–13+

Table 3: Cyber safety topics

In many cases videos were part of a series of videos, and as such it is important that such a series of videos is kept and used together. Based on these assessments, three syllabus tables, one for each age group, were drafted. Each of these syllabus tables (Tables 4 to 6) reflect a lesson number, a main topic area or video focus and the URL of the video. It will be noted that videos that form a series are grouped together with the same numerical lesson value, but different alphabetical characters.

It is suggested that teachers spread these lessons over a period of six or even twelve months to periodically instil the required cyber safety lessons and messages. Following below are the tables showing the three syllabuses: Table 4 for 7 to 9 year olds, Table 5 for 10 to 12 year olds and Table 6 for learners of 13 years and older.

Children ages 7–9		
	Topic areas	**URL**
Lesson 1a	Basic cyber safety	*http://www.youtube.com/watch?v=-nMUbHuffO8*
Lesson 1b	Summary of Lesson 1a	*http://www.youtube.com/watch?v=vmqNg-7QrDk*
Lesson 2a	Sharing personal information	*http://www.youtube.com/watch?v=M-njh8mFvVk*
Lesson 2b	Summary of Lesson 2a	*http://www.youtube.com/watch?v=VhThfiQ7FRA*
Lesson 3	Hector's World 1	*http://www.thinkuknow.co.uk/5_7/hectorsworld/Episode1/*
Lesson 4	Hector's World 2	*http://www.thinkuknow.co.uk/5_7/hectorsworld/Episode2/*
Lesson 5	Hector's World 3	*http://www.thinkuknow.co.uk/5_7/hectorsworld/Episode3/*
Lesson 6	Hector's World 4	*http://www.thinkuknow.co.uk/5_7/hectorsworld/Episode4/*
Lesson 7	Hector's World 5	*http://www.thinkuknow.co.uk/5_7/hectorsworld/Episode5/*
Lesson 8	Hector's World 6	*http://www.thinkuknow.co.uk/5_7/hectorsworld/Episode6/*

Table 4: Syllabus for learners of 7 to 9 years of age

Children ages 10–12		
	Topic areas	**URL**
Lesson 1a	Phishing and viruses	http://www.youtube.com/watch?v=svb6d55e29k
Lesson 1b	Information on web not always true	http://www.youtube.com/watch?v=GNf3OmUKWmk
Lesson 1c	Sharing personal information	http://www.youtube.com/watch?v=HiyqFwXnMZo
Lesson 1d	Cyber bullying	http://www.youtube.com/watch?v=ipD0IS4EUcI
Lesson 1e	Summary of above	http://www.youtube.com/watch?v=HI0US7LgGeQ
Lesson 2a	Protect password	http://www.youtube.com/watch?v=T0Q5b-pzhD8
Lesson 2b	Do not open suspicious files	http://www.youtube.com/watch?v=nlx4wRkssRo
Lesson 2c	Beware of online friends	http://www.youtube.com/watch?v=j88SddAk--I
Lesson 2d	Tell a trusted adult	http://www.youtube.com/watch?v=oXNsXKgJw0c
Lesson 2e	Cyber safety rules	http://www.youtube.com/watch?v=xp9H01BKL2Q
Lesson 2f	Summary of above – Part 1	http://www.youtube.com/watch?v=MDvhiwMwdO4
Lesson 2g	Summary of above – Part 2	http://www.youtube.com/watch?v=E3vVbAitTDY
Lesson 3a	Accepting friend requests	http://www.youtube.com/watch?v=KGr_KFiCX4s
Lesson 3b	Privacy settings	http://www.youtube.com/watch?v=-Dn1Jmqecvk
Lesson 3c	Cyber bullying	http://www.youtube.com/watch?v=elYv-pZVgyo
Lesson 4a	Do not meet online friends in real life	http://www.youtube.com/watch?v=gPse7dcXwrU
Lesson 4b	Online game addiction	http://www.youtube.com/watch?v=hGfjyDALM2Q
Lesson 4c	Illegal downloads	http://www.youtube.com/watch?v=N1xFUw3bW10
Lesson 4d	Cyber bullying	http://www.youtube.com/watch?v=RKi9FybL-Og

Table 5: Syllabus for learners of 10 to 12 years of age

Children ages 13+		
	Topic areas	**URL**
Lesson 1a	Accepting friend requests	http://www.youtube.com/watch?v=KGr_KFiCX4s
Lesson 1b	Privacy settings	http://www.youtube.com/watch?v=-Dn1Jmqecvk
Lesson 1c	Cyber bullying	http://www.youtube.com/watch?v=elYv-pZVgyo
Lesson 2a	Online privacy	http://www.youtube.com/watch?v=vYIfnjgn_eY
Lesson 2b	Cyber bullying	http://www.youtube.com/watch?v=Hfi881lONSk
Lesson 2c	Sharing of private information	http://www.youtube.com/watch?v=vijhpQsxnQM
Lesson 3	Think before you post information online	http://www.youtube.com/watch?v=dT1GvPQG904&list=PLB5E270C7C30E3079
Lesson 4a	Safe social networking	http://www.youtube.com/watch?v=Esj-PBmXjCU
Lesson 4b	Cyber privacy	http://www.youtube.com/watch?v=9bhHaVxo3i0
Lesson 4c	Cyber bullying	http://www.youtube.com/watch?v=xGKmlTtZnSk
Lesson 4d	Online postings can haunt you in the future	http://www.youtube.com/watch?v=V3DlVkOAPVQ
Lesson 4e	Be careful of online friends	http://www.youtube.com/watch?v=y4nyluaXoFY
Lesson 5	Sexting	http://www.youtube.com/watch?v=AL5Y6rJwTuQ

Table 6: Syllabus for learners of 13 years and older

It should be noted that each of the three tables above reflect a number of publicly available online videos most suitable to the ages mentioned. The content and basic cyber safety message(s) of each of these videos are clear and self-explanatory. It is recommended that the teacher, before presenting the lesson to the class, look at the video and identify its main message. It would be easy to find more related information, from Google for example, on the topic to prepare the teacher for some discussion with the learners afterwards. It would be ideal if the video lesson were discussed as a group afterwards. A discussion will ensure that the cyber safety message is clearly understood by the learners and subsequently entrenched.

As mentioned earlier, no lesson plans or discussion questions are included in each of the lessons and the individual teachers will have to contextualise the message based on their individual circumstances. It was clearly not the objective of this paper to prepare a fully-fledged syllabus with lesson plans and associated learning and discussion material, but it should be noted that the Hector's World environment has a complete set of such material available, ready for the teachers to use (Think_U_Know, 2008). On the other hand, the authors and the expert teacher are of the opinion that the attached 'syllabus tables' can be used with much success in any classroom.

From a technical point of view, it is obviously important that the teacher is able to show the individual videos to the class using an Internet link, a computer and ideally a data projector with audio. If a computer facility is available, the children can watch the videos individually or in groups of two or three. None of these videos are longer than 10 minutes; therefore the time to stream them should be reasonable even if the Internet connection is fairly slow. It was also found that Google Chrome was the best browser for viewing the videos.

7. Conclusions

Cyber space is growing by the day. More and more services appear in cyber space every day and more and more people are becoming absolutely dependent on cyber space for entertainment, social networking, e-commerce, finding information etc. It is also known that, along with all these advantages of cyber space, a number of ever-increasing risks are present. For this reason it is important that the users of cyber space should be properly schooled in using these services in a secure and safe manner. Internationally, many governments are taking the lead or at least ensuring that some form of cyber safety or security training is conveyed to their general population, whether young or old, private or professional, as everybody needs to be cyber smart to protect themselves as well as commercial and governmental assets. Most countries envisage a cyber safe culture as the ultimate goal in this regard.

Although Africa in general is seen as a developing region, it is important to note that Africa is active in cyber space and similar cyber safety awareness and education programmes are just as applicable to Africa as to the rest of the world. It is also noted that very few African countries have really introduced organised and coordinated

measures for ensuring such a cyber safe culture. In few schools in Africa such efforts are taking place.

Although everybody active in cyber space needs to be made aware of the risks and be educated on ways and means to protect themselves, this paper set out to address the specific needs of young, primary school learners. The objective of this paper was to identify some publicly available online resources, which can be used in a class situation by a teacher to educate and train young 7 to 13 year old learners. Three different 'syllabus tables' were prepared for three different age groups. Each of these syllabus tables present a set of videos with cyber safety related messages in a genre most applicable to that particular age group involved. Using these, teachers should be empowered to play an important role in preparing and equipping primary school learners for their activities in cyber space.

8. Acknowledgement

The input and contribution of Mrs Hester von Solms, an experienced teacher, is hereby acknowledged.

9. References

ACOPEA. (2012). "African Child Online Protection Education \& Awareness Centre," *available online from: http://www.cto.int/media/events/pst-ev/2013/CTO%20Forum/African%20Child%20Online%20Protection%20Education%20\&%20Awareness%20Centre.pdf, Accessed on [12 November 2013].,* 2012.

Antwi-bekoe, E., and Nimako, S.G. (2012). "Computer Security Awareness and Vulnerabilities : An Exploratory Study for Two Public Higher Institutions in Ghana," *Journal of Science and Technology,* vol. 1, pp. 358-375, 2012.

Atkinson, S., Furnell, S.M., and Phippen, A. (2009). "Securing the next generation: enhancing e-safety awareness among young people," *Computer Fraud \& Security ,* vol. 2009, no. 7, pp. 13-19, 2009.

Becta. (2009). "AUPs in context: Establishing safe and responsible online behaviours," *available online from: http://education.qld.gov.au/studentservices/behaviour/qsaav/docs/establishing-safe-responsible-online-behaviours.pdf, Accessed on [10 November 2013].,* 2009.

Byron, T. (2008). "Safer Children in a Digital World," *available online from: http://webarchive.nationalarchives.gov.uk/20130401151715/https://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf, Accessed on [5 November 2013].,* 2008.

Cole, K., Chetty, M., Larosa, C., Rietta, F., Schmitt, D.K., and Goodman, S.E. (2008). "Cybersecurity in Africa : An Assessment," *available online from: http://s3.amazonaws.com/zanran_storage/www.cistp.gatech.edu/ContentPages/43945844.pdf, Accessed on [22 November 2013].,* 2008.

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

Dlamini, I., Taute, B., and Radebe, J. (2011). "Framework for an African policy towards creating cyber security awareness," *Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW),* pp. 15-31, 2011.

e4Africa, "Technology in schools – for better or for worse," *available online from: http://www.e4africa.co.za/?p=3516, Accessed on [20 November 2013].,* 2011.

Grobler, M., and Dlamini, Z. (2012). "Global Cyber Trends a South African Reality," *IST-Africa 2012 Conference Proceedings,* 2012.

Jisc. (2012). "A guide to open educational resources," *available online from: http://www.jisc.ac.uk/publications/programmerelated/2013/Openeducationalresources.aspx Accessed on [20 November 2013].,* 2012.

Kanyesigye, F. (2013). "New drive to fight hackers, New Times," *available online from: http://www.newtimes.co.rw/news/index.php?a=66437&i=15343, Accessed on [22 November 2013].,* p. 2013.

Kortjan, N., and von Solms, R. (2013). "Cyber Security Education in Developing Countries: A South African Perspective," *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering,* vol. 119, pp. 289-297, 2013.

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

Mars, M., and Erasmus, L. (2012) "Telemedicine can lower health care costs in Africa," *Innovate,* vol. 7, pp. 32-33, 2012.

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

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

OER Africa. (2013). "Understanding OER," *available online from: http://www.oerafrica.org/understandingoer/UnderstandingOER/tabid/56/Default.aspx, Accessed on [20 November 2013].,* 2013.

PWC. (2012). "Telecoms in Africa: innovating and inspiring," *Communications Review,* 2012.

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

Safaricom. (2012). "iCow," *available online from: http://www.safaricom.co.ke/personal/value-added-services/social-innovation/icow, Accessed on [12 November 2013].,* 2012.

Safaricom. (2012). "Relax, you've got M-Pesa," *available online from: http://www.safaricom.co.ke/personal/m-pesa/m-pesa-services-tariffs/relax-you-have-got-m-pesa, Accessed on [12 November 2013].,* 2012.

Sato, N. (2013). "ICT stakeholders discuss emerging issues on African cyber security," *available online from: http://www.humanipo.com/news/32773/ict-stakeholders-discuss-emerging-issues-on-cyber-security, Accessed on [21 November 2013].,* 2013.

TeleGeography, "Africa's international bandwidth growth to lead the world," *TeleGeography: Global Bandwidth Forecast Service,* 2013.

Think U Know. (2013). "Welcome to Hector's World," *available online from: http://www.thinkuknow.co.uk/5_7/hectorsworld/, Accessed on [15 November 2013].,* 2008.