

CENTERIS 2012 - Conference on ENTERprise Information Systems / HCIST 2012 - International
Conference on Health and Social Care Information Systems and Technologies

The Integration of Information and Communication Technology in Schools. Online Safety.

Elisabete Pires^a, Fernando Moreira^{a*}

^a*Universidade Portucalense, DICT, Porto, Portugal*

Abstract

The Information and Communication Technologies (ICT) in the context of education present important opportunities integrated not only in school curricular and non-curricular activities, but also in organizational ones. For students the experiences with these technologies include Internet network accesses and all the potentialities and challenges that they present. Here we also have to consider the dangers and threats. These accesses are performed partly within the school and largely outside the school environment.

Schools have an important role in the discovery and learning of the use of these technologies.

This article is based on a study conducted in schools which aimed at the understanding of how ICTs are integrated and relate to the educational community. The study tried to understand the functioning of facilities and security measures, access to information, solutions and procedures implemented by schools. It also tried to put some future possibilities into perspective.

© 2012 Published by Elsevier Ltd. Selection and/or peer review under responsibility of CENTERIS/SCIKA - Association for Promotion and Dissemination of Scientific Knowledge Open access under [CC BY-NC-ND license](#).

Keywords: Information and Communication Technologies; information systems; online security; online ethics.

* Corresponding author. Tel.: +351225572372; fax: +351225572000.
E-mail address: fmoreira@upt.pt.

1. Introduction

1.1. The context of ICT in schools

Schools are complex organizations consisting of a diverse community of teachers and students, integrated in a specific socio economic and cultural context as is reported in Lobe et al. [1], and Livingstone and Haddon [2].

Teachers usually come from different areas of knowledge and most of them do not master ICT tools. Sometimes there is need to support them in developing abilities to use these tools in teaching contexts. ICT skills are required in education not only due to their inevitable presence, but also because of the transversal nature they possess, Ministério da Educação [3].

Moreover, these technologies should take into account the information systems of the schools and the availability of information about the students, teaching resources and administrative systems.

Thus, ICTs have a transversal use in school, covering the various academic and non-academic teaching activities in their various aspects: curricular, teaching, recreational and administrative tasks.

In school activities, students are stimulated to use ICTs to research, present and publish project works, to communicate and interact [4-5].

In a report of the project *EU Kids Online 2009* [7] on the use of the Internet and the integration of ICT in schools it can be read that: “*Greater internet use is associated with higher levels of education, so educational achievement may be expected to increase the extent and sophistication of internet use. Further, gaps in ICT provision and insufficient/ outdated provision of ICT in schools should be addressed, and media education should be recognised and resourced as a core element of school curricula and infrastructure.*” Livingstone and Haddon [2].

1.2. The problem of online security in schools

Technologies provide young people with opportunities and benefits; however, they also expose them to risks which they may not be prepared to handle. Apparently, there is a relationship between the increase of online experiences and digital capabilities, and exposure to these risks, as well as the ability to deal with them [6].

Online activities which may be considered of risk may include contact with strangers, the availability of personal data, access to sites with misleading or inappropriate content for the age of these young people and unethical actions such as access to illegal downloads and cyber bullying, [2, 8]. These actions require monitoring and guidance which should have continuity beyond the school environment, once it appears that accesses outside of school are superior to those made within school environments, [6, 8]. In addition, with the development of mobile devices, the monitoring of these accesses has become increasingly more complicated or impracticable [6].

Bearing in mind the scope of this issue and the involvement of people to whom it is addressed, the application of security technologies and information systems developed and implemented should be considered taking into account not only the diversity of the community but also the actions proposed.

In Livingstone and Haddon [2], aspects such as the page design, appropriate legislation and implementation, and the intervention of service and content providers are focused.

In this report there can be read “Children can only be supported in managing the online environment if this is substantially regulated – by law enforcement, interface and website design, search processes, content and service providers, online safety resources, etc”.

The report published in 2011, also refers to the fact that the increase of Internet use by children presents other challenges to all the intervenient in the development of Internet content, particularly in the development of educational activities which are challenging, creative and use language appropriate to the age of the audience. This report concludes by presenting some recommendations for governments, the industry, the educators, the parents, the society and other entities with responsibility [6].

In the field of warning and prevention of the dangers on the Internet, there are several projects being developed in Portugal and elsewhere which focus on the notion that in addition to a targeted and efficient use of new technologies in classrooms there should also exist an orientation to a safe and responsible behavior on the Internet, inside and outside the schools. Projects like SeguraNet [10], Insafe [11] and MiudosSegurosNa.Net [12].

In order to have an updated and contextualized understanding of this subject in schools, a study focusing on the integration of ICT in education was developed.

This way, considering the schools, the people and the processes, the study tried to access the resources used and the implementations of ICTs in their different aspects: procedures for monitoring and preventing online dangers, control and organization of the school curriculum and available information, knowledge and practices of teachers facing the challenges that these technologies present to them, security technologies and procedures used by schools and also students' awareness of online safety.

The study also tried to obtain an opinion of the teachers involved in activities of collaborative nature and online projects, on the knowledge of students, parents and guardians, on the issue of online security and possibilities for the development of knowledge and higher involvement of the educational community.

This paper presents the approach used to access the schools and information based on the methodology of the study and the data obtained in the sample. It presents the main results according to the three aspects discussed in the study: schools, people and processes from the point of view of ICT and online security. It also presents the main conclusions and recommendations for those involved in this issue.

2. The Research Framework

2.1. Methodology and sample

The study based itself on a qualitative methodology for it was believed that this was the most suitable approach to explore poorly studied issues or issues presenting many unknown factors. Each school participating in the study was considered as a case study.

The total number of the schools involved in the study tried to achieve a representation at national level not forgetting the scope of the study. Thus, it was tried that teachers who represented these schools and answered the survey would be related to ICT in schools through their functions, subjects or the development of projects with students. Not all teachers who participated in the study were in the area of computer science, and it was found out that there are schools without teachers in this specific area.

After a first approach to schools through traditional mail and email, an approach was made through social networks related to the subject of the study, with the aim of increasing its representativeness.

The study focused itself on basic schools because these schools face, at the moment, a strong expansion of applications in the context of computing according to the technologic plan of education and by the ministry of education, Ministério da Educação [3]. In these schools, the students also correspond to the age range of young people important to online monitoring, [2, 6].

The sample comprised 22 schools.

2.2. *Collecting and presentation of data*

The method used to obtain the testimonies was based on a semi-structured interview available online, first via email and later through a service that enables the provision of online forms.

The data were organized and the analysis of the main results and conclusions is presented below.

3. **Research Findings**

The data were organized based on the three aspects that the study focused, i.e., security technologies and information systems in schools, the relationships of people and the educational community with these technologies and the processes implemented by schools aiming at online security.

3.1. *The integration of ICT in schools*

Many schools seek control and security solutions in addition to antivirus, filtering and blocking, and they look for wider systems which can inclusively develop other functions including resource management and access.

Regarding the availability of resources and educational content, data and other information about activities, students, staff and other administrative information, many schools use the eLearning platform Moodle – Modular object oriented dynamic learning environment – an Open Source Course Management System platform or Learning Management System.

This platform is easy to access and manage for the user. As a content management system it offers some control over the access to the information provided and it allows some degree of privacy and security, providing degrees of priorities through the functions assigned to users and administrators and password access.

As for other administrative information management and access control of the data and of other sites, this platform is not very developed. It doesn't also present ways to control access outside its scope.

However, as a platform for eLearning many schools seem to rely on this application for providing educational content and other information related to students and the functioning of the school, in a safe way.

With a more ambitious nature and with more defined objectives in the area of security there is the Inspirus Project, which consists of an application based on software installed on Magalhães computers, namely the Magic Desktop [13], whose aim is to create a controlled access to applications and the Internet. This software was developed by the company EasyBits in partnership with Intel and it now attempts to present three controlled work environments: home / family, the school network and the classroom, allowing the definition of the tools to be used in each of the environments. The program is based on a server that enables the user to define the type of tasks and applications that students can perform allowing the teacher to control the activities of students on the computers and making it possible to define in real time the tools that students can use. This software works only on Windows platforms, this features are described in Casa dos Bits [14].

Another school in this study presented the project edgeBOX [15], which allows control and management of information in a more integrated and comprehensive way.

The edgeBOX solution was developed by Critical Links, a company dedicated to developing and implementing solutions in the area of Information Technology (IT) and communication networks with integrated voice, data and security. This solution concentrates functions which are typically distributed by various devices and generate cost savings, space and need for management.

Critical Links is part of the consortium led by Portugal Telecom which won the international public competition launched by the Ministry of Education to create Local Area Networks in schools within the Technological Plan for Education.

Besides the integration of services and maintenance and management of networks, this solution enables remote monitoring of the network through an access browser.

This solution presents several modes of implementation allowing settings to a local or wide area network and the implementation of a Virtual Private Network.

The firewall can be customized and users can be required to authenticate themselves in order to access services. Thus, the school that reported this implementation can control the Internet access by the students, even those using laptops, as they are registered at the points of access via a MAC address and are thus subjected to the Web filtering of the school, whether they are Linux, Mac or Windows. However, this process does not resolve the situations in which students access the network through their own Internet access.

However, a problem mentioned by the school is that students try to work around these controls and filtering by using proxy servers.

3.2. ICT and people

The fact that teachers are educated in the area of computer expertise can help them in technical issues but this fact does not imply that there has been training in online security.

Figure 1 shows the results of the study. In this study the cases were separated according to the following criteria: teachers who integrated the projects belonged only to the group of teachers educated in computer sciences, teachers who integrated the projects were educated in the group of computer science and other areas and teachers who integrated the cases were educated only in other areas.

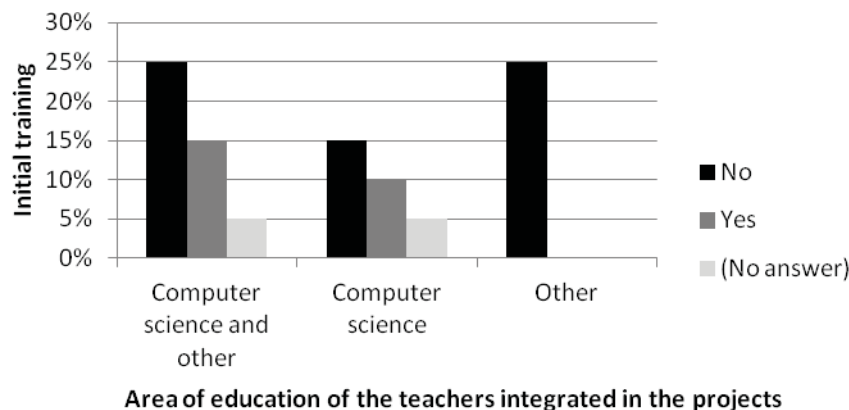


Fig. 1. Area of education of the teachers integrated in the projects and initial training in online security.

On the other hand, this is an issue that needs to be treated transversally, regardless of the levels of education and curriculum area of the teachers.

Thus, training in this area is considered an important factor for many teachers, although some consider that they already have the necessary expertise.

Being the area of education of the teachers not a relevant factor, the knowledge of security technologies is and will always be of utmost importance.

The testimony of a school considered its system quite safe and having a good control and management of access and information. It is a school without teachers in the area of IT but where the edgeBOX project was implemented and the teacher responsible for it was trained along with the implementation of the project.

These implementations require investment in technologies and training and an approach which must involve the whole school community.

In fact, it appears to be consensual that this training should be extended to parents, since many of the accesses to the Internet are made outside of school. However, this training should be adjusted to the local community allowing everyone to feel interested and having the opportunity to participate.

3.3. The security procedures in schools

Apart from choices of schools in terms of security technologies and community involvement in education, the access to mobile devices is quite widespread, regardless of the socio-cultural context where the school is included, as shown in Figure 2, and this fact brings additional difficulties to monitoring and security.

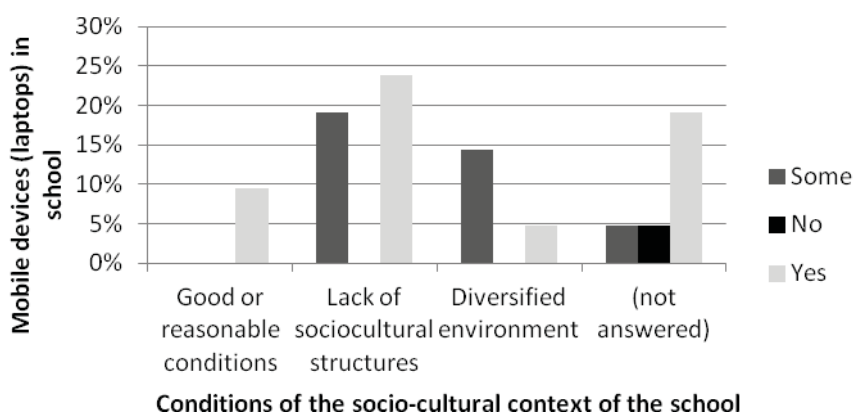


Fig. 2. Conditions of the socio-cultural context of the school and mobile devices (laptops) in the school.

Monitoring places with internet access, in and out of schools, becomes more difficult as it relies mainly on staff with supervision functions, monitoring, password access and antivirus software. But it appears that there is some lack of overall supervision and protection of access in certain locations.

It was also observed that although there is the feeling that students are aware of this issue, there are still many doubts and the notion that there are risky behaviors, especially in the sharing of personal information in social networks.

Apart from technologies, the presentation of projects in this area has had an important action in the transmission of information and development of some activities.

In fact, raising awareness in schools is based mainly in the presentation of projects in this area, mostly through posters and some activities included in the classes.

Figure 3 shows the most popular tools used by teachers integrated in the projects mentioned in the study. The projects of presentations in this area are also included. As before, data for teachers included in the

projects, only of the area of education of computer science, computer science and other areas and other areas only are presented.

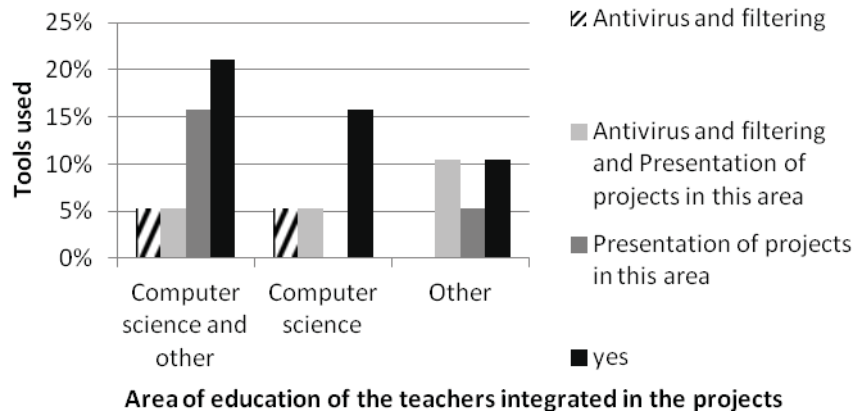


Fig. 3. Area of education of the teachers integrated in the projects and tools used.

In this study, some schools also mentioned the need for the equipment to be appropriated and having updated programs.

Finally, it is also important to note that certain rules of conduct and information presented in the regulation book of the school, as mentioned in some testimonies, can be a starting point to call attention and foster discussion on issues concerning the safety and proper use of ICT in schools.

4. Conclusions and Future Works

The implementation of ICTs and information systems in schools should involve several aspects related to information management and control of access. Some steps towards this could involve the availability and access to educational content, management of data concerning students or access to intranet and the Internet.

The access to the Internet by students requires some precautions that schools seek to address through surveillance and registration. The existence of mobile devices has added difficulties to this control.

In addition, aspects related to the protection and orientation of young people when they are on the Internet must be integrated into school activities and the information systems must be prepared for this.

In some cases, schools seek more specific and comprehensive systems which usually involve an investment in resources and training.

As the schools are integrated in a diversified environment and suffer influences from the outside the implementation of ICTs or an information system should involve teachers, students and the whole school community and it should also take into account the specific context where the school is located.

In what regards teachers, their involvement and training are essential to the implementation and use of security technologies and information systems in schools.

With regard to young people, in addition to schools and parents, these aspects should be considered by all those responsible for Internet access and content development.

Thus, the access control systems to computer networks and the Internet should be supervised by individuals and entities with responsibilities in guiding young people.

The information and training, together with the inclusion of technology, will always be the most important path to follow. This path should be balanced and focused and it should involve an analysis of each situation, so that implementations can achieve the desired results.

This is an area that given the diversity and dynamics of the environment where it operates presents challenges for information systems.

The applications still require further development and integration in schools and they will only be possible with the involvement of the educational community, the society, the industry, and the agencies with responsibility in controlling the development of applications, legislating entities and other entities.

This work would also imply a monitoring and analysis of developments and results.

This study has discussed the projects implemented in schools which cooperated in this research and it has discussed possibilities for further developments and implementations.

In the future, it would be interesting to conduct a broader analysis of the results obtained involving the collaboration of more schools. It would also constitute an interesting follow-up of this study to monitor the implementation of other projects and analyze their integration and results.

In what regards the involvement of parents, it would also be important to develop activities to raise awareness and engage parents and guardians in monitoring the access of children to the Internet, teaching them how they could improve the supervision of their children. Similarly, it would also be important to verify the development and the reactions to these activities by the parents and the community involved.

References

- [1] Lobe, B., Livingstone, S., Haddon, L., 2007. Researching Children's Experiences Online Across Countries: Issues and Problems in Methodology - EU Kids Online, <http://eprints.lse.ac.uk/id/eprint/2856>
- [2] Livingstone, S., Haddon, L., 2009. EU Kids Online: Final Report. London School of Economics and Political Science, [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20\(2006-9\)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf)
- [3] Ministério da Educação, 2007. Despacho nº 16 149/2007 de 25 de Julho, Diário da República, 2ª Série, nº 142, p. 21077. Lisboa, <http://dre.pt/pdfgratis2s/2007/07/2S142A0000S00.pdf>
- [4] Amante, L., 2007. Infância, escola e novas tecnologias. In "As TIC na educação em Portugal - Concepções e Prática", Costa, F. A., Peralta, H., Viseu, S., Orgs. Porto Editora, pp. 102-123.
- [5] Baltazar, N., 2004. Crescer com a Internet: Desafios e Riscos, Actas do III SOPOCOM, VI LUSOCOM e II IBÉRICO –Volume IV, www.bocc.ubi.pt/pag/baltazar-neusa-crescer-internet-desafios-riscos.pdf
- [6] Livingstone, S., Haddon, L., Gorzig, A., Ólafsson, K., 2011. EU Kids Online Final Report. The London School of Economics and Political Science, LSE, [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/EUKidsOnlineIIReports/Final%20report.pdf](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf)
- [7] EU Kids Online, <http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>
- [8] Tito de Moraes, 2011. Como Proteger Crianças e Jovens Destes Riscos Online?, [MiudosSegurosNa.Net](http://www.miudossegurosna.net/), <http://www.miudossegurosna.net/>
- [9] Willard, N., 2006. A Briefing for Educators: Online Social Networking Communities and Youth Risk. Center for Safe and Responsible Internet Use, CSRIU, <http://csriu.org/cyberbully/docs/youthriskonlinealert.pdf>
- [10] SeguraNet, <http://www.seguranet.pt/blog/>
- [11] Insafe, <http://www.saferinternet.org/web/guest/home>
- [12] MiudosSegurosNa.Net, <http://www.miudossegurosna.net/>
- [13] Magic Desktop, <http://www.magicdesktop.com/pt/>
- [14] Casa dos Bits, 2010. Inspirus quer conquistar espaço nos computadores das escolas, Tek, http://tek.sapo.pt/noticias/computadores/inspirus_quer_conquistar_espaco_nos_computado_1047293.html
- [15] Critical Links - edgeBOX, <http://www.edgebox.com/opencms/opencms/critical-links-uc.html>