Digitalization of education: challenges and opportunities

‘Digital citizenship is character education in this networked world’

I Secure Consortium
Preface

Young people and children are amongst the biggest user groups of ICT in Europe, with about 75% of the children frequently using Internet\(^1\) (EC DG Communications Networks, Content & Technology, 2013; London School of Economics, 2009). In order to stay safe, they need to be trained about both online opportunities and risks. This publication describes the development of the products of the I Secure project towards the promotion of Internet security skills and competences in secondary schools, in particular. As such, this publication is intended for teachers of secondary schools as well as for ICT experts working in the field of education, parents and students.

\(^1\) Survey of Schools: ICT in Education, EC DG Communications Networks, Content & Technology, 2013. 
EU Kids Online, London School of Economics, 2009
Acknowledgement

The work presented in this publication has been co-funded by the Erasmus+ Programme of the European Union, under the action for Strategic Partnerships for school education, and directly supported by the Agenzia Nazionale Erasmus+ (INDIRE) representing the Erasmus+ Programme in Italy for the actions aimed to school education.

We would like to express our sincere thanks towards the partners who devoted their time and knowledge for the past three years in the development, implementation and quality assurance of this project.

We are especially indebted with the schools, teachers and experts who willingly participated in the activities of the project to test, validate and promote the results, ensuring the quality of the productions and assessing the viability of implementing it into the school education system.
Executive Summary

I-Secure: “Empowering Education Systems in Information Security” is an Erasmus+ Project that promotes the strategic and safe use of information and communication technologies in teaching and learning programmes as a precondition for the development of innovative practices at secondary school level (students of 11-18 years).

I-Secure project brings together 7 partners from 5 European countries (AT, BG, ES, IT, NL), forming a transnational cooperation partnership with a balanced geographical representation of the Erasmus+ area. The aim of this publication is to present a summary of the project outputs and the key conclusions and recommendations addressed to the most relevant stakeholders of this project: secondary school teachers, headmasters and students.

The main Project Results are:

1. Needs and Gaps Analysis: a desk research for identifying the concrete problems and challenges and for collecting examples of good practices and innovative didactical practices and methodologies in the field of Information Security.

The field research addressed mainly students and secondary school staff (headmasters and teachers), but it also involved parents, policy makers, local representatives, third sector, etc. in order to identify the target groups’ training needs on Information Security education.
The main Survey results indicate the need to develop a strategy, at school level, on Information Security education, and identify the different training needs of teachers, school staff, students and parents.

2. “I-Secure Agent” Prototype: a professional qualification including training curriculum and materials to enable teachers to become “I Secure Agents”, being able to transfer the course contents to students within their daily teaching activities.

The **I-Secure Agent European Professional Qualification** (Recommended EQF certification Level 4) is designed based on the results of the needs analysis and is composed of the following core units of learning outcomes:

- Unit 1 – Protection against incorrect and aggressive behaviour in social networks and personal information protection;
- Unit 2 – Elements of Security System (firewall, antiviruses, contactless devices);
- Unit 3 – Intellectual Property Rights for Digital Content and ethical behaviour in the legal context

The I-Secure Agent training course has been implemented in a customized version of Moodle, a Learning Management System online platform.

3. **TEL I-SECURE Eco-System**: represents the I SECURE system for learning activities and collaborative creation of content. It includes several ICT tools as “ready to use” learning instruments available for teachers to foster an informed and aware use of ICT tools in educational activities.
The Consortium has implemented an online learning space composed by multiple components (communication tools, training aids, open resources and ad hoc resources) that are in an interactive and complementary relation. These different components define the space where to adapt open learning: where to share teaching resources through open licenses for Open Educational Resources (OERs).

The online course and Platform have been tested in order to assess the adequateness and effectiveness of the “I-Secure Agent” training course contents and to test the TEL I-Secure platform with end users to identify any technical and methodological issues.

The testing phase took place in the four Partner countries (Bulgaria, Italy, Spain, The Netherlands) where the partners organised respectively four National training events and collaborative learning activities.

The heterogeneity of the group which included teachers and headmasters perfectly matched with the project aim of promoting the strategic and innovative use of ICT at school level through the involvement of the main players (teachers) and the final beneficiaries of education (students).

The testing results revealed the success of the initiative both, at a single country level and at European level, because of the partnership composition and regional distribution that covered the main European regions.

**Recommendations and Conclusion**

Finally, recommendations are provided to teachers, students, parents, school managers and policy makers.
The I-SECURE Project demonstrates that specific training through open online courses for teachers and school staff in particular can represent a successful approach for enhancing their effective role in student education in the current digital learning environment.

The project results are a starting point for a more comprehensive approach to the digitalization process in school education. All the different parties involved (policy makers, teachers, school staff, students, parents) demonstrated a high level of interest and engagement for future initiatives on this topic.
Table of Contents

Partnership ........................................................................................................................................... 9
1. Introduction ........................................................................................................................................ 10
   1.1 I SECURE Project: aim, objectives and results ........................................................................ 11
2. Needs & Gaps Analysis .................................................................................................................... 13
   2.1 Methodology and tools .............................................................................................................. 14
   2.2 Target group ............................................................................................................................. 15
   2.3 Needs & Gaps Analysis Results ............................................................................................... 16
   2.4 Conclusion and Recommendations .......................................................................................... 21
3. 'I Secure Agent' European Professional Qualification ................................................................. 23
   3.1 Course structure and contents .................................................................................................. 24
4. TEL I SECURE eco-system ............................................................................................................. 30
   4.1 IT Architecture of the Platform .............................................................................................. 31
5. Testing phase ..................................................................................................................................... 35
   5.1 Testing structure and objectives ............................................................................................... 36
   5.2 Testing activities and tools ........................................................................................................ 37
   5.3 Results of National testing and consultation activities ............................................................ 40
6. Recommendations and Conclusion ................................................................................................. 43
   6.1 To teachers ............................................................................................................................... 44
   6.2 To students ............................................................................................................................... 46
   6.3 To parents ................................................................................................................................... 47
   6.4 To schools’ managers ................................................................................................................ 48
   6.5 To policy makers ....................................................................................................................... 49
Conclusion .................................................................................................................................................. 51
**Partnership**

I Secure project brings together 7 partners from 5 European countries, forming a transnational cooperation partnership with a balanced geographical representation of the Erasmus+ area.

Partners bring important experiences in the field of education and information security in school education, as well as teacher training and ICT based learning methodologies and instruments.

The project coordinator is USR – Educational Department of Lazio Region, Italy. Another Italian partner is EFFEBI - Finance & Banking Association for Organizational Development and Human Resources. The two companies included in the consortium are ECOSTUDIO - ICT training organization from Italy, and Inercia Digital S.L., Spain. Two universities are also included in the partnership - Open University of Netherlands and UNWE – University of National and World Economy, Bulgaria. The project evaluator is MERIG – European Research Institute, Austria.
1. Introduction
1.1 I SECURE Project: aim, objectives and results

‘Empowering education systems in information security’ - I Secure - is and Erasmus+ Project that promotes the strategic use of information and communication technology in teaching and learning programmes as a precondition for the development of innovative practices at secondary schools level (students of 11-18 years), in four Partner countries (Bulgaria, Italy, Spain, The Netherlands).

The Project aims to:

a. Implement methodologies and tools for the professional development of teachers in the field of Information Security
b. Promote the 'Information Security Culture' to increase the awareness in this field as a crucial step in the digitization process of the educational contexts.

The main Project results are:

a. Needs and Gaps Analysis: a desk research to identify the concrete problems and challenges and for collecting examples of good practices and of innovative didactical practices and methodologies in the field of information security.

b. “I Secure Agent” Prototype: a professional qualification including training curriculum and materials to enable teachers to become 'I Secure Agents', being able to transfer the course information to students within their daily teaching activity.
c. TEL I SECURE eco-system: represents the I SECURE system for learning activities and for collaborative creation of contents. It includes several ICT tools as 'ready to use' learning instruments available for teachers to foster an informed and aware use of ICT tools in educational activities.

d. Stakeholders are also provided with Guidelines for using the TEL I SECURE eco-system in order to facilitate its valorisation and further exploitation in the Partner countries and abroad.

These results were piloted and validated during the project piloting phase and were fine-tuned and are all available online, on the project website.
2. Needs & Gaps Analysis
2.1 Methodology and tools

Partners conducted the Analysis through online Questionnaires, Interviews and Focus Groups conducted at national level in the four Partner countries with various stakeholders.

In order to facilitate the comparison, the analysis and the evaluation of the information collected at European level, a common methodology and investigation/reporting tools have been designed.

In particular, the analysis was focused on five topics, selected by the Partners, related to the Information Security education:

- Widespread and protection of personal information: personal data; digital identity; procedure/rules on digital signatures for sending/receiving documents, etc.
- Communication on social-networking sites, cyber-bullying and unfair behaviour (CBUB)
- Elements of security systems (firewall, anti-spyware systems, VLAN etc.) and a safe internet use (activation of anti-virus, anti-spam systems etc.)
- Acquisition and use of digital creative contents on the Internet: concepts of Intellectual Property Rights (IPR); rules/measures of control for the respect of IPR; how to verify the quality/validity of information collected on internet (source) etc.
- Risks for the health connected to the use of Wi-Fi and wireless devices (e.g. position of server, rooter at home and also within schools etc.).
2.2 Target group

The field research addressed mainly students and secondary school staff (headmasters and teachers) but it also involved parents, policy makers, local representatives, third sector, etc. in order to identify the target group’s training needs on Information Security education.

A total number of 440 stakeholders in the four Partner countries took part in the different analysis activities.

Interviews were addressed to middle and secondary school staff (teachers, headmasters) to understand their training needs related to the five above mentioned topics in the field of Information Security education. Furthermore, the interviews represented also an opportunity to identify other relevant information on existing National Policies / Strategies promoted by Public Authorities concerning the Information Security education in schools.

In addition, Partners had the possibility to collect information regarding schools’ initiatives and the current challenges to be addressed.

The Focus Groups involved school staff, students and parents, and also local stakeholders as representatives of local authorities, policy makers, trade unions, researchers, parents’ associations, third sector etc.

Due to the participation of a larger variety of actors in the Focus Groups, it was possible to validate the results emerged in the national surveys and interviews, and also to identify the further training needs of the target groups, not only related to the schools’ organizational constraints, but also to the local/national context.
2.3 Needs & Gaps Analysis Results

Based on the results of the survey, the main results indicate the need to develop a strategy, at school level, on Information Security education aiming at:

- Organise regular and structured training courses for teachers on ICT security, at different levels of complexity, according to their needs, in order to update and boost their knowledge and skills;
- Deliver teacher training mainly through schools and using instruments that allow self-learning;
- Deliver innovative educational tools, more attractive for students and useful for the educational process;
- Make available, within the schools, trained personnel in the technical management of ICT (security) tools in order to support and assist teachers during the lectures;
- Increasing the number and variety of learning opportunities dedicated to ICT security;
- Updating the educational programme based on innovative pedagogy and ICT tools that could be more motivating for students (e.g. learning by serious games);
- Supporting students in developing critical mind-set and emotional intelligence in order to manage properly their emotions on internet (especially in relation to Cyber-bullying and unfair behaviour on social networks) establishing “educational network” with students’ parents since most of the behaviours towards and on internet are also linked to the student’s family culture, background and values.
- Organize school initiatives (workshops, training courses etc.) on themes such as the strategic and
secure use of the Internet also with the involvement of parents.

Training needs - School staff

The main training needs identified by the school staff responding to the I SECURE survey are related to:

- Communication on social-networking sites, cyber-bullying and unfair behaviour (CBUB) on the Internet;
- Safe Internet use;
- Basic concepts on how to access secure information, content and data, defend privacy, digital identity and physical protection;
- How to protect computers, devices and connections from malwares and not authorized accesses;
- Security related to the communication (e-mail, instant messages).

Training needs - Students

The findings of the Needs & Gaps Analysis demonstrate that although students have some knowledge regarding Information Security, their behaviour shows that it is necessary to train them further not only on theoretical data, but also on adopting a correct approach to this topic. Educating students how to behave in a digital environment, in fact, also requires teaching them some rules regarding honesty, ethics, respect, and citizenship and applying training strategies to emotionally engage them.

In particular they expressed a particular interest for the following topics:
• Widespread and protection of personal information
• Cyber bullying and unfair behaviour on social networks
• Elements of Security Systems and Safe Internet Use
• Acquisition and use of digital creative contents on the Internet
• Risks for the health connected to the use to Wi-Fi and wireless devices.

In addition, other two key elements have been identified regarding students’ training needs in Information Security:

• To train also their behaviour by implementing training strategies that engage them also emotionally
• To educate them that digital environment should follow also specific rules regarding honesty, ethics, respect, citizenship

Training needs - Parents

Although parents seem to have some information regarding Information Security, it is necessary to provide them a complete and structured training covering all five topics identified within the project, as well as some support in understanding the students’ psychological approach to ICT and the Internet, in particular.

Considering the findings of the survey, it is evident that most often the computer is placed in spaces “visible” to the parents - the living room and study room.

However, it is not clear to which extend parents are monitoring their sons’ activity at the computer and on the Internet, since the survey results show that generally parents do not support their children in the Internet usage and 37% of parents declare that they place a computer in the sons’ bedroom.
This behaviour could be related to the existence of transparent and effective communication within the family regarding their activity on the web.

A positive finding is also the fact that parents seem to be quite aware of some risks children are exposed to: cyber-bullying and visiting inappropriate/dangerous websites are at the top of the list.

In addition, parents need to have the knowledge and the instruments to replace the ‘don’t do it’ with a concrete and positive support for their children for using the Internet safely.

This approach will both improve the communication between parents and their children and will impact on students’ effective behaviour towards ICT and Information Security in particular.

Moreover, during the interviews conducted, Partners could identify some more challenges and actions to be undertaken to support the information security in middle / secondary schools:

- Develop school programmes on Information Security Education in line with the National strategy;
- Provide, at national level, the necessary software tools to be used by schools;
- Provide a national portal for the collection of good practices, e-learning tools and serious games to be used as case studies in the educational process;
- Organize regular (at least one per year) training courses for teachers on Information security Education
(online courses with practical exercises and guidelines);
• Organize national “Olympiads” for students on Information security Education (school competitions for best results, e.g. through the realization of video-clips on Information security);
• Develop online courses for students on correct behaviour against cyber-bullying and unfair behaviour on Internet;
• Create, within the school website, a section dedicated to the information security (best practices; tools; latest security treats and related information etc.).

In order to support the teachers’ training on Information security, the following items have been identified:

• New trends on Information security problems (the newest and biggest treats);
• New tools for protection against unfair and incorrect behaviour on Internet – guidelines on how to use and install them;
• Good practices and guidelines on how to design serious games on Information security;
• Offline and online training materials on new challenges in Information security.

Ultimately, the main results of the Focus Groups demonstrate that although the national contexts are rather different, there are some key common topics considered relevant by the participants:

a. The importance to support knowledge sharing with concrete and interactive learning experiences for
students, such as serious games and sharing of experiences;
b. The need to engage also parents in order to have a stronger impact on students’ behaviour regarding the Internet;
c. The need to focus the education on Information Security not only on technical information, but mainly on students’ correct behaviour on the web since many risks are connected to this issue.
d. The opportunity to create cooperation tools for teachers for facilitating knowledge and experience sharing.

2.4 Conclusion and Recommendations

School staff, students and parents commonly recognize the importance of improving the involvement of their schools in the field of information security education by providing training courses for them or organizing awareness campaigns and workshop activities with the participation of experts, students’ parents, financial policy, local representatives and other relevant stakeholders.

In particular teachers, as educators, feel responsible of students’ learning and are motivated to acquire and transfer to their students more information / culture on the topic.

They also agree on the importance of having an Information Security Education course curriculum, as compulsory subject within school programme, supported by an effective educational strategy at school level, better if developed in coordination with national Policies.
In addition, the implementation of collaborative activities on this topic will represent an opportunity for schools for establishing an “educational alliance” with families, which is fundamental for fighting incorrect behaviours on internet. Parents have to be aware that family education is important as well as school education.

Taking into consideration the training needs identified for the target groups, Project Partners, with the support of the school staff and experts involved in the interviews and focus groups, have proposed a possible structure and contents for the definition of course curriculum for the staff training programme:

Module 1: Protection against incorrect and aggressive behaviour in social networks
Module 2: Antiviruses
Module 3: Configuration of software-based firewall
Module 4: Intellectual Property Rights for Digital Content

The overall analysis results demonstrate that most of respondents, among school staff, students and parents of the four participating countries, are rather aware of their limited knowledge and competences on the main aspects of the information security education. They are convinced that schools, supported also by Public Institutions, have to be the first educational channel on this topic.
3. ‘I Secure Agent’ European Professional Qualification
3.1 Course structure and contents

The I Secure Agent European Professional Qualification was developed on the basis of the training needs of the project target population, identified and analysed in the Intellectual Output (IO) 2 – Needs & Gaps Analysis. The ‘I Secure Agent’ European Professional Qualification (Recommended EQF certification Level 4) was designed on the following core units of learning outcomes:

- Unit 1 – Protection against incorrect and aggressive behaviour in social networks and personal information protection;
- Unit 2 – Elements of Security System (firewall, anti-viruses, contactless devices);
- Unit 3 – Intellectual Property Rights for Digital Content and ethical behaviour in the legal context.

Add some info about the ECVET points – what are they and according to which criteria we attributed them

Table 1.
Units’ structure, lessons’ contents and relative learning tool

<p>| Unit 1. Protection against incorrect and aggressive behaviour in social networks and personal information |
|---|---|---|
| Lesson title | Type | ECVET |
| 1. Define the basic approach to identify risks related to private information and personal information protection on the web | Serious game | 0,50 |
| 2. Identify and describe unfair behaviour on social networks (part 1 and 2) | Video lesson | 1 |
| 3. Implement and define safety | Video | 0,50 |</p>
<table>
<thead>
<tr>
<th>Communication while using ICT devices</th>
<th>Lesson</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total of ECVET</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Unit 2. Elements of Security Systems</strong>&lt;br&gt;(firewall, anti-viruses, contactless devices)</td>
<td></td>
</tr>
<tr>
<td>1. Identify and list the most common Malware</td>
<td>Webinar</td>
</tr>
<tr>
<td>2. Develop the strategies for networks security</td>
<td>Interview</td>
</tr>
<tr>
<td>3. Implement strategies for networks security</td>
<td>Moodle Workshop</td>
</tr>
<tr>
<td>4. Describe and implement security tools</td>
<td>Video Lesson</td>
</tr>
<tr>
<td>5. Illustrate and analyse strategies for using Internet safely</td>
<td>Video Lesson</td>
</tr>
<tr>
<td>6. Develop strategies for password management</td>
<td>Assignment</td>
</tr>
<tr>
<td><strong>Total of ECVET</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Unit 3. Intellectual Property Rights for Digital Content and ethical behaviour in the legal context</strong></td>
<td></td>
</tr>
<tr>
<td>1. Understand Intellectual Property: patents, copyrights, trademarks and trade secrets basic principles of IPR</td>
<td>Video lesson</td>
</tr>
<tr>
<td>2. Outline cyberspace and Intellectual Property Rights</td>
<td>Moodle Workshop</td>
</tr>
<tr>
<td>3. Explain the benefits of Intellectual Property</td>
<td>Video lesson</td>
</tr>
<tr>
<td>4. Understand and avoid Misunderstanding of IP Usage</td>
<td>Moodle Workshop</td>
</tr>
<tr>
<td>5. Open Source and creative commons - variable licenses</td>
<td>Interview</td>
</tr>
</tbody>
</table>
Here in the following each unit contents are described.

**Unit 1 – ‘Protection against incorrect and aggressive behaviour in social networks and personal information protection’** focuses on:

- Notions related to the risks in management and sharing of information and data on the Internet
- Legal definitions and distinctions of the different unfair behaviours that can be faced by using social networks (e.g., Cyber-stalking, Trolling, Traditional bullying);
- Notions on psychological and social consequences/effects of unfair behaviours on youngsters (e.g. Intimidation, emotional damage, suicide, etc.);
- National policies and strategies regarding unfair behaviours on social networks.
- Practical examples and strategies to handle unfair behaviour (e.g. through multimedia channels, games, search engines and pop culture);
- Action plan for handling unfair behaviour (e.g. awareness campaigns, bilateral meetings, workshops, etc.);
- Risks involved with sending and receiving e-mail messages (Spam, Phishing, Wrong identities, dangerous attachments, dangerous links contained) and instant messaging apps.
- Techniques to protect private and personal data in online services using personal computers and mobile devices.
Unit 2 – ‘Elements of Security System (firewall, anti-viruses, contactless devices)’ presents:

- How to recognize computer affected by malware;
- Implement strategies to protect computers, devices or networks from malware and unauthorized access;
- The most common types of network and wireless security;
- How network security works (operation) and its components (Anti-virus and anti-spyware; Firewall, to block unauthorized access to your network; Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks; Virtual Private Networks (VPNs), to provide secure remote access);
- Safe use of contactless devices;
- Strategies to protect computers with anti-virus, firewall and personal hotspot;
- Practical information and strategies on:
  - Set up a high protection level of privacy for Internet navigation
  - The family navigation setting
  - Browse in private with incognito mode: implications
  - What cookies and pop up are
  - What to avoid while using open WIFI connection in public places
- Principles on safe passwords management.

The last unit, Unit 3 – ‘Intellectual Property Rights for Digital Content and ethical behaviour in the legal context’, aims at delivering the following knowledge:

- Patents;
- Copyrights;
• Trademarks;
• Trade Secrets basic principles of IPR;
• Ethical aspects and issues of IPR;
• Legislative notions of privacy ethic on the Internet;
• Ethical use of New Media;
• Use of IP;
• Functioning of the World Intellectual Property Organization;
• Example of good usage of IP;
• Common misunderstanding of IP Usage;
• Plagiarism;
• Different license models of creative commons licenses.

Because of the great responsibility that teachers have against students as educators and as bridge between parents and students, the Professional Qualification mainly addresses secondary school teachers.

The training course wants to be flexible, open and organic in order to assure individual and group interaction and exchange of contents, resources and meanings. Subsequently the key objectives of the I Secure course are engagement, ubiquity, connectivity and socialisation of competences, values and networks. The learning and delivering methodology reflects that these prerogatives have the potential to enable individuals to enhance the social dimension of learning.

**Delivering methodology**

The I Secure Agent training course is distributed as a MOOC (Massive Online Open Course) which means a set of contents organised in a course, freely accessible on the
Internet with a large capacity in terms of participants and delivered on an online platform.

**Learning methodology**

The adopted methodological approach includes a mixing of methodologies which range from the traditional learning to e-learning and distance learning which will be reflected also into a variety of teaching tools such as video lessons, interview, webinar, serious game, forums, chat and wiki.

**Assessment methodology**

At the beginning of the course there is a pre-assessment questionnaire, a self-assessment to establish that the participant possesses ad adequate entry level for the course which corresponds to the EQF Level 3. At the end of each unit there is an assessment quiz in order to verify the comprehension of the unit and at the end of the course, the users access to a final evaluation questionnaire. Not only questionnaires, but also other kind of evaluation tools such as assignment and peer-to-peer evaluation were adopted.
4. TEL I SECURE eco-system
4.1 IT Architecture of the Platform

Within the I Secure project, a learning ecosystem has been developed based on the principles of Technology enhanced learning (TEL). This first expression needs some clarifications on what is meant by learning ecosystem and how we implemented a TEL strategy.

A learning environment consists of a wide set of features that affect learning. The combination of technologies and learning resources available in a given environment is a learning ecosystem.

TEL is often used as a synonym for e-learning but can also be used to refer to “learning with technology”, rather than just through technology. In other terms, the TEL encouraged the use of technology to maximise the student learning experience and to guarantee even a flexible approach to open learning. Technology itself offers potential flexibilities in what is learned, how it is learned, and where it is learned. It can provide numerous ways to access resources and information and to interact with teaching staff and learners.

Within the I Secure project, the Consortium has implemented an online learning space is composed by multiple components (communication tools, training aids, open resources and ad hoc resources) that are in an interactive and complementary relation. These different components define the space where to adapt open learning: where to share teaching resources through open licenses for Open Educational Resources (OERs). The design of the technology infrastructure for online learning had to take into account the desire to create a MOOC, a Massive Open Online Course. In terms of instructional design models to be employed, MOOCs can be
classified into two distinct types: xMOOCs (Extended MOOCs) and cMOOCs (Connectivist MOOCs).

The difference between extended and connectivist MOOCs is related to where learning takes place. xMOOCs are designed to be run in a single MOOC platform that can handle many concurrent users. On the contrary, the key concept behind cMOOCs is networking, meaning that learners may go anywhere to locate sources of information. Learning may also take place outside the official MOOC platform.

Within the I Secure project, the xMOOC model has been adopted. The I Secure Extended MOOC provided all the information and the learning activities in a structured linear order, followed by self-assessments designed to check whether the particular learning objectives of the MOOC course had been achieved.

The architecture
The use of technology within the TEL strategy takes into account these objectives:

a. Support a massive use of resources and their open access
b. Create a Teaching and Learning strategy taking into account the xMOOC structure
c. Meet student expectations and improving their satisfaction
d. Establish a common user experience for TEL services
e. Create a student learning experience and engagement strategies

Fig. 1 The architecture of I Secure TEL ecosystem
The Learning Management System Moodle is the main component of the learning system. It represents the core of the virtual learning environment. Moodle is used for managing users and educational resources (courses, OERs Archive, etc.) as well as for the creation of non-formal pathways of learning. Moodle, in fact, covers the Forum and includes the Wiki module for the co-design of teaching materials and OERs.

Among the educational resources, Moodle allows the presence of videos, podcasts and WBT, web-based training. On the technological component of TEL I SECURE ecosystem, the provision of services has been ensured through the integrated use of the following sections and
related application, through the mechanisms of SSO (single sign-on):

**Core Module Realized With Moodle**

- Educational area: this area provides lessons and formal training
- Administrative area: User and content management thanks to the Moodle modules
- Information area within Moodle: OER repository and teaching materials.

**Social Module**

- Collaborative area: social networking and content co-creation.

**Personal Learning Module**

- e-Portfolio

**Game Module**

Serious game tool: Partners designed a serious game, representing a key learning instrument available within the eco-system. Branching stories are ICT-based means that take the form of trees with branches of alternative evolution paths. Being built just like a tree, every choice taken is a different branch, with a different ending and a different impact in terms of pedagogical objectives. This applies also to trainers alike, as the switch to a personalized learning and competence-based assessment is a big challenge.
5. Testing phase
5.1 Testing structure and objectives

The testing phase is aimed at assessing the adequateness and the effectiveness of the contents of the “I Secure Agent” training course and at beta-testing the TEL I Secure platform with end-users in order to identify the presence of any technical and methodological issues.

As a result, the piloting phase represented a crucial part of the I SECURE project as it allowed the examination of the two main outcomes of the project:

- The “I Secure Agent” European Professional Qualification for Teachers
- The virtual collaborative learning platform TEL I Secure Eco-System.

In order to ensure the achievement of the two goals – the assessment of the training course and the technical check of the platform – the testing phase was structured in two stages:
Stage 1: O5/A2.National training event
The National training event was a face to face pilot conducted through training modules with teachers whose aim was the assessment of the training course’s contents.
Stage 2: O5/A3.Collaborative learning activity on ‘social networking’
The collaborative learning activity on ‘social networking’ was an online pilot through a collaborative learning exercise whose aim was the test of the TEL I Secure Eco-System platform and its contents.
5.2 Testing activities and tools

National training events

The testing phase took place in the four Partner countries (Bulgaria, Italy, Spain, The Netherlands) where partners organised respectively four National training events and four collaborative learning activities. The National training event was aimed at introducing the TEL I Secure Eco-System and evaluating the ‘I Secure Agent’ curriculum in terms of:

- Structure of the three modules
- Lessons’ contents
- Learning methods: blended learning, virtual classroom, e-learning, distance learning
- Learning tools/instruments: video lessons, interview, webinar, serious game, forums, chat and wiki
- Assessment methods: questionnaires, assignment, peer evaluation (Moodle workshop)
- ‘I Secure Agent’ Professional Qualification.

At the beginning of the National training events a Pre-Assessment Questionnaire was distributed among the participants in order to self-assess the involved participants.
on their ICT knowledge and their previous experience and interest in IT Security. The Questionnaire was composed by: - closed questions with a ranking scale from 1 to 5, being 1 the lowest rate and 5 the highest; - closed questions with YES/NO answer; - a multiple choice question to choose the topics/modules teachers are more interested in.

After the presentation of the two main Project’s results, an Evaluation Questionnaire was then distributed at the end of the event. The Evaluation Questionnaire was aimed at generally evaluate the event and collect feedbacks and suggestions from the audience. The Questionnaire, in fact, included a set of questions where the audience should express its general satisfaction, rating it on a scale from 1 to 5, being 1 the lowest rate and 5.

**Collaborative learning activity**

The Collaborative learning activity, instead, was an online activity which was conducted in the four Partners’ country (Bulgaria, Italy, Spain, The Netherlands) in order to validate both the ‘I Secure Agent’ Professional Qualification in terms of learning outcomes and contents and the TEL I Secure Eco-System platform with its functionalities. In this way, the Collaborative activity supported the Consortium with the identification of potential improvements in terms of course curriculum (learning outcomes, teaching methodology and tools, learning contents) and technology of the relative platform (usability, bugs, performance issues etc.).

Furthermore, the implementation of a collaborative activity enhanced the creation of an active virtual learning community of teachers.
The validation process was conducted in an asynchronous way in order to concretely test the course, the effective usability of the platform and the creation of an open learning environment.

The users were asked to register and navigate for one month (15 February – 15 March 2018) the ‘I Secure Agent’ course and the TEL I SECURE Platform with the support of one technical tutor from ECO Studio e-learning and a didactical one from UNWE, USR Lazio, Inercia and OUNL.

At the end of the testing activity, learners were required to fill in an Evaluation questionnaire whose completion was mandatory to receive the Certificate of attendance.

The Evaluation Questionnaire was distributed both in online version (Google Form) and in paper version and was structured in a set of closed questions with a ranking from 1 (the lowest) to 4 (the highest) and two open questions aimed at evaluating:

- Learning outcomes
- Teaching methodology and tools
- Learning contents
- Usability of the platform
- General satisfaction of learners and tutors.

**Target group**
The identified target group included a minimum of 15 testers/Partner country whose agreed profile had to be mainly lower and upper secondary school teachers. Nevertheless, in the spirit of the I SECURE Project, also other profiles related to the educational and school environment (e.g. headmasters, supervisors, students, parents etc.) were involved into the testing in order to
promote a constant dialogue with these stakeholders on IT security at school. The selection of participants was based on the following criteria:

- From lower and upper secondary level school (11-18 years)
- Disciplines: equal distribution among humanistic, scientific and technical disciplines
- Age and sex: equal distribution of age and sex range to have and heterogeneous group
- Teaching experience: 3 years
- Knowledge: generic knowledge on IT Security
- Competences: generic digital competences
- Good English level

5.3 Results of National testing and consultation activities

In all countries the continuous communication and dissemination of the Project with the same stakeholders guaranteed not only a general interest in the Project’s progression but also a constant involvement of these actors and, subsequently, it allowed the participation of at least 15 testers per country.

The heterogeneity of the group which included teachers and headmasters, supervisors, students, parents perfectly matched with the project’s aim of promoting the strategic and innovative use of ICT at school level through the involvement of the main players (teachers) and the final beneficiaries of education (students).

The selection process of the participants allowed the
identification of a group of teachers with a good level of confidence with IT since around the 70% of the target group assessed its ICT competences as pretty advanced and only the 27% (mostly in The Netherlands) felt to have basic skills.

Such a competence, in addition to a previous general experience in online courses granted a good level of familiarity and interest in the topics of the Professional Qualification also because mostly none of the involved participants took part to a MOOC in this field.

The ‘I Secure Agent’ course, in fact, gained a favourable consensus among its audience: not only the course was defined to be very well structured in terms of learning outcomes and contents but also profitable for the course’s final users (the teachers) who felt to have improved their professional skills and relevant for enhancing the digitalization of education programmes in schools.

Also the TEL I SECURE Platform received very positive feedbacks for its architecture and variety of tools and activities. The presence of technical and didactical tutors contributed to the effective functioning of the Platform and guaranteed the suitable support to the users.

In conclusion, the testing results revealed the success of the initiative, both at the single country level and also at European level because of the partnership composition and regional distribution that covered the main European regions.

However, as this phase was aimed at concretely test the course and the platform, this activity not only demonstrated its goodness, but also helped the Consortium in identifying eventual room for improvements:
a. provide training course also for lower levels of the qualification (e.g. EQF level 3)
b. integrate further examples and case studies directly linked to the educational context
c. correlate the Platform also with some social networks
d. provide translated version of the MOOC
e. develop complementary course for parents and students.
6. Recommendations and Conclusion
6.1 To teachers

Teachers play a very key role for students’ education and even more this crucial role becomes relevant with regards to Cybersecurity.

As students spend most of the day at school, teachers have the possibility to observe their students’ behaviour with technology and eventually intervene in order to correct any misleading attitude.

However, in order to make the teachers’ intervention effective, it is necessary that teachers become aware of their role with regards to ICT Security.

Such a change in considering technology as a benefit can be achieved following these recommendations:

Create/Get involved in cooperation networks and activities for teachers for facilitating knowledge and experience sharing on ICT

Being part of a community that shares the same interest on a topic or that at least shares the same goal – improve ICT knowledge and skills – can be very supportive for two main reasons:

Firstly, teachers are stimulated and motivated in improving their professional career, acquiring new competences or updating old ones.

Secondly, being part of a collaborative network, teachers can support each other with their experiences, creating a supportive environment based on mutual trust, confrontation and discussion on topics they are interested in.
This learning community can be created with the support of some tools like social networks and online forums which assure a bottom-up approach that directly involve all committed teachers who are interested in this topic or workshops and seminars for teachers on ICT security which, if organised in cooperation with school managers or teachers’ associations, can allow a great level of confrontation and discussion on innovative pedagogical practices.

Establish an “educational network” with students’ parents

Since most of the behaviours towards and on the Internet are also related to the education, background and values that students have received within their families, an agreed strategy and a combined intervention by teachers and families could be very effective for students as it will facilitate not only their comprehension and awareness of the risks of the Internet but especially the development of the “emotional intelligence” in terms of honesty, ethics, respect, citizenship.

Students need to be supported in developing critical mindset and emotional intelligence in order to manage properly their emotions on the Internet (especially in relation to Cyber-bullying and unfair behaviour on social networks).

Such a reflection can be triggered in students with some activities that can stimulate the emotional involvement of the student like the usage of role games or serious games.
6.2 To students

Students are the greater consumer of technology within the educational panorama as all their daily routine is characterized by the use of several devices and the access to the Internet.

Despite this, the relation between the time that students spend on the Internet and their awareness of the correct use of these tools or of the correct behaviour to adopt in these virtual environments shows a serious gap where there is a need for intervention by policy makers, families and schools.

Apart from a proper ICT education students should receive from parents and schools, it is crucial for the establishment of a healthy relation with technology that students follow two main recommendations:

Be aware of the ‘reality’ of the Internet

The Internet offers a lot of opportunities to keep in contact and share with others and friends ideas, photos and to access to a lot of information. However, students need also be conscious of the ‘dark side’ of the Internet. Accessing to Internet, in fact, it is not only a game but it also implicates responsibilities, and it requires students to be careful to:

- Fake news and resources they can have access to as they can violate Intellectual Property Rights;
- Potential frauds can be received by emails;
- Photos posted online or chat as they may be offensive or violate others’ privacy.
Ask for help

The Internet can be a very disorienting place without the right indications to live within and this may lead students to isolate themselves when they face any issues or they feel to be in a dangerous situation.

Asking for help can be difficult but it is the only way to exit from a distressing situation.

6.3 To parents

Family is the first place where children access technology and where the relation with the Internet is established. Such a presence in the children’s life requires parents to be correctly informed on ICT tools to correctly stimulate their sons. Technology cannot be a taboo rather an occasion of confrontation and discussion where parents play the crucial role of mediator between the Internet and their children.

In order to play this role, parents need to keep in mind two recommendations:

Include ‘ICT education’ as part of the educational background

ICT education needs to be considered as part of the educational package that young people needs to have in order to correctly approach to technology. Young people should not be left alone with technology but since the early moments they enter in contact with any technology it is necessary to educate them to its correct
usage. With relations to technology, parents need to be aware of the use of technology their sons do as it will guarantee a more transparent relation within the family and also a enhance discussion on such a topic. Family discussion represent a crucial part for young people character’s development as it allows confrontation and the definition of an own mind-set that needs to be oriented at initial stage.

**Be a model**

Only if parents’ relation with technology and the Internet is healthy, their children will do the same. Being a positive model is the only strategy parents have to educate correctly educate children in all the sphere of their lives and the same should happen with ICT.

However, being a model cannot implicate a total refuse of technology by parents and a subsequent ban for the children: technology can be a barrier but also a bridge to enforce the relations between parents and sons.

### 6.4 To schools’ managers

As technology belongs to everyday life in school, it is important that schools have relevant tools and strategies to promote a positive use of ICT but also to prevent and intervene when problematic situations occur.

Among different perspective, two main recommendations can be underlined:
Develop an e-Policy

School should state and describe within their policy also which is its vision on e-safety and in particular which are the initiatives to promote ICT skills and competences among students and teachers. School should inform about rules and procedures to be applied for accessing to ICT within the school, to prevent incorrect usage of technology.

Promote transversal initiatives on digital education for students and teachers

Involving schools into different and transversal projects related to digital education can give an added value to the school’s offer not only because the school staff is motivated and supported in working and taking initiatives on this topic, but also because it guarantees a spread of information between students and teachers.

6.5 To policy makers

Policy makers are directly involved into the challenge launched by technology to education as they can be the catalyser for a revolution of digitalization in schools.

Such a responsibility implicates national policies and strategies of intervention to both support teachers and students in opening the education process to technology.

As a result, policy makers should:

Develop and support initiatives on Information Security Education
The digitalization of education needs the direct intervention of policy makers who have the resources to start a virtuous cycle that can benefit both teachers and students. In order to concretely consider cybersecurity as a priority, policy makers should support and promote initiatives aimed at enforcing Information Security Education addressing both teachers like the development of ITE and CPD compulsory courses on ICT and students like transversal activities (workshops, MOOCs etc.)

**Enhance ICT infrastructure in school education, together with appropriate training of teachers and school staff**

According to a European Commission’s survey (2013)\(^2\) in schools there are on average between three and seven students per computer in the EU. Around 50% of students use a desktop or a laptop during lessons at least weekly, but around 20% of them never or almost never use a computer during lessons. As a result, ICT equipment (especially interactive whiteboards and laptops) is insufficient for all students and is considered the major obstacle to effective ICT use in schools. Policies and action at infrastructure level are necessary in order to digitally equip schools and students with laptops (or tablets, netbooks, etc.) and interactive whiteboards. Such a policy, however, can only positively impact only if linked to a complementary training of teachers and school staff.

**Provide a national portal for the collection of good practices, e-learning tools and serious games to be used as case studies in the educational process**

---

As ICT Security needs to be implemented at school level on the national territory, in order to ensure a wider spread of the ‘culture of information security’ and to allow a continuous discussion and update on this topic, it would be useful to develop a national database for good practices and relevant case studies that can be consulted by all interested parts and that can offer resources and materials already tested to be replicated for supporting the learning process.

Conclusion

In the digital era technology cannot be considered as an alien component of education and it requires to be integrated as a necessary resource in order to understand students’ needs, to catch their attention and interest and to transmit relevant ICT skills or experience that can enrich students’ professional background and smooth the school-work transition.

School staff and parents have a full responsibility in educating students in correctly approaching to technology and can apply several strategies.

I SECURE Project demonstrates that specific training through open online courses for teachers and school staff in particular, can represent a successful approach to enhance their effective role in student education in the current digital learning environment.
This kind of initiative contributed to improve the level of confidence of teachers with ICT and subsequently their ICT knowledge and skills. Furthermore, the networking activities allowed the creation of a learning community that, even if virtual, supported users into the learning process.

The project’s results represent a starting point for a more comprehensive approach to the digitalization process in school education. All the different parties involved (policy makers, teachers, school staff, students, parents) demonstrated a high level of interest and engagement for future initiatives on this topic.