18-07-2017

Deliverable D6.1
Study of Security, Privacy, Identity Management and Legal Requirements in the Digital Schools' Environment Using a Cloud-Based Approach

Deliverable 6.1

Contractual Date:	30-06-2017
Actual Date:	18-07-2017
Grant Agreement No.:	732049 – Up2U
Work Package:	WP6
Task Item:	Task 1
Nature of Deliverable:	ORDP (Open Reseacrh Data Pilot)
Dissemination Level:	PU (Public)
Lead Partner:	GARR
Authors:	Andrea Corleto, Eleonora Napolitano, Giorgio Valente, Vincenzo Puglia, Andrea Pinzani, Gabriella Paolini, Marco Malavolti, Davide Vaghetti, Donatella Cesareni, Domingo Docampo Amoedo, Vicente Goyanes De Miguel, Mary Grammatikou, Ilias-Stylianos Karabasis, Stefano Lariccia, Marco Montanari, Iván Otero González, Nadia Sansone, Peter Szegedi, Antonis Vekris

The innovation action leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 732049 – Up2U.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This deliverable is the starting point of UP2U project's investigation of the landscape of security, privacy, identity management and legal requirements within the digital schools' environment using a cloud-based approach [1].

ICT use within a school-based learning context deals not only with the tools pupils and teachers choose for their lessons: what Learning Management System or file-sharing system they decide to run, if they browse the web with computers or just download data (such as files or images) with smartphone apps, it also deals with diverse issues about ICT security, the network, operating systems and applications. ICT security is a very critical aspect and there is a strong need for schools and the higher education system to have a better understanding of the context: what kind of threats and weaknesses schools face and what related countermeasures apply to protect network infrastructure. School staff (principals, teachers, ICT officers, etc.) all need to be involved in a public discussion on common best practices for security protection to improve understanding of the gaps to be filled.

Furthermore, ICT and network security are the on-off switches to assure data protection and privacy. New European legislation, the General Data Protection Regulation (Regulation EU 2016/679), in effect from 25 May 2018, will replace the current Directive and will be directly applicable in all member states. GDPR covers Internet communication and strengthens data protection: personal data may be processed only in specific cases. The education system must be prepared to changes needed by GDPR rules, in particular with regard to online activity: how do schools manage their students' information? Where are stored data? Who can access them?

One of Up2U's goals is to set up a common framework for schools' identity and access management (IAM). Within the context of secondary schools (pupils between the ages of 11 and 19), this generation completely fits the definition of digital natives: "living lives immersed in technology". To live a life fully-merged with technology, students manage several digital identities. This immersion also applies to learning.

Moving on from the analysis of students' emerging behavioural trends regarding digital identities in higher education, this paper aims to provide a coordinated approach to enable enduring and scalable IAM solutions.

The last point that this report considers is intellectual property and the utilisation of Open Educational Resources (OER). The use of OER in educational courses, through resource-based learning, is proportional to the ease of use of digitised resources and multimedia objects in particular, via the Internet. Resource-based learning should not be thought of as an alternative to replace traditional

education (classroom-based); rather, by enabling the friendly use of digital technology to facilitate the learning process through different media, resource-based learning constitutes a complementary form of teacher-student interaction, which is bound to become a key component of any formal education programme.

1 Introduction

While discussing UP2U project proposal, we all agreed on the phrase “Educational Ecosystem” to identify the context in which learning really happens, whether in structured, formally organised institutions (formal learning), or outside of these formal institutions, including personal, interpersonal or community-based transactions about information, knowledge, and competencies that happen informally.

The term ecosystem is a concept used by life sciences, but more and more applied to social and educational science as well. Education is often defined, from a philosophical point of view, as a superior faculty of social-based adaptation of humans to their environment.

Within the Up2U project, the educational ecosystem is composed of:

- Actors (learners, teachers, mentors, as well as digital assistants such as bots, automata).
- Knowledge objects (books, digital books, digital content)
- Infrastructures (classrooms, laboratories, shelves, desks; virtual rooms, virtual repositories, virtual desks and virtual laboratories).

As a team of pedagogic experts and technicians, there is awareness of the need to create (or adopt) a comprehensive and shared taxonomy to effectively cooperate in implementing a prototyping model with demonstrative functionalities on how a modern ecosystem should work at the service of education, learning, and learners.

Main overall goal should be to liberate creativity within learning environments, where the interleaving of stimuli and responses alongside the interplay of actors and tools is becoming increasingly complex. The goal of freeing creativity and prejudice-free thinking is the destination where the system's stakeholders should be nudged.

In summary, the more technology-driven infrastructures that adopt, the greater awareness and creativity we should stimulate and obtain in our educational communities [2].

1.1 Aim of the Survey and Methodology

The main ambition of the Up2U project is to use a bottom-up strategy to help schools, where teachers as well directors/administrators play an active part in the project itself. Two surveys were drawn up with an aim to collect data and experiences from the school protagonists: teachers and directors. Surveys were carried out via Google Forms because of its affordability and its simplicity.

Schools were quite cooperative in responding to the surveys. Indeed, most of them were already part of Up2U as pilot school or as candidates to be pilot schools in another stage of the project. Two surveys to understand pilot schools' needs, to be able to focus on them, to give them the best solution.

The first survey collected useful information about the schools participating in the project, covering five main areas:

- School technological resources for teaching.
- School involvement in innovative and cross-collaborative projects.
- State of the art of teacher training.
- Teachers' attitude towards technology-enhanced collaborative learning.
- Teachers' perceptions about students' skills.

Through these areas, it was possible to organise information needed to structure an effective learning path, take into account resources and constraints, teachers' expectations and needs, and to serve UP2U's goal to better connect with schools and universities. Such information was especially useful for partners directly involved with pilot schools.

Two versions of the survey were drafted versions: one for head teachers/principals (bullet point 1 and 2) and one for teachers (bullet point 3, 4 and 5). Each survey contained a set of questions and Likert responses (scored along a range) and a series of open-text questions, where respondents could add free comments.

The second version of the survey, aimed at schools, is the most useful for providinga current snapshot of the situation in schools around Europe, including: ICT security concerns, new issues for privacy and identity management, incoming legal requirements requested by the new European legislation on data protection (GDPR) and some notable remarks on intellectual property rights and Open Educational Resources.

Structured by the leading Working Package (WP) with an interdisciplinary workgroup, the survey has been distributed online in English, with a Google Form link [3], in the UP2U project's pilot countries. The survey was made available for input from 1 to 18 June 2017, and collected 55 responses from schools in six countries: Greece, Hungary, Italy, Lithuania, Poland and Spain. Based on over 60 questions, the survey aimed to have a direct and concrete feedback from schools, although it has limited statistical value due to the restricted sample size.

The main areas of investigation were:

- General information
- Personal data
- ICT infrastructure and services
- Security
- Identity Management

- Intellectual property
- Privacy

Survey questions were based on a mix of open-ended and closed-ended questions in order to provide an indication of the awareness of respondents, as well as the level of schools' ICT and network infrastructures. Submitted surveys provided qualitative response on several issues such as new GDPR, data protection and identity management, as well as quantitative estimates to report a real–time picture.

The survey focused on head teachers/principals, teachers and IT assistants of ISCED Level 2 Lower Secondary Education) (27.3% of respondents) and Level 3(Upper Secondary Education) (72.7% of respondents) State-funded schools. 63.6% of them are male and 36.4% are female and they are distributed by age as follows: 43.6% between 40 and50; 32.7% between 50 and 60; 18.2% between 30 and40; 3.6% over 60; 1.8% between 20 and 30. The percentage of respondents per country is Greece (16.4%) Hungary (12.7%) Italy (12.7%) Lithuania (9.2%) Poland (43.6%) and Spain (5.4%).

Some interesting responses detail ICT infrastructure and services area. It should be noted, above all, that information systems are mainly managed by school staff: 32 responses out of 55 (58.2%) by teachers; 27 responses out of 55 (49.1%) by IT assistant; 12 responses out of 55 (21.8%) by head teachers/principals; 3 responses (5.4%) on "Other", with only one of these reporting a "private external service". Other remarkable outcomes are listed below in Table 1.1.

QUESTION	YES	NO	DON'T KNOW
Does the school's internet connection meet your needs?	81.8%	18.2%	-
Is your school connected to the National Education and Research Network (NREN)?	27.3%	34.5%	38.2%
Does your school have a network traffic segregation policy physical or logical?	63.6%	20%	16.4%
Does your school have WiFi?	92.7%	5.5%	1.8%
Does your school have public IP addresses?	61.8%	20%	18.2%
Does your school have a firewall?	81.8%	9.1%	9.1%
Does your school use a Network Address Translation (NAT)?	58.2%	7.3%	34.5%

Table 1.1: Network infrastructure

41 respondents out of 55 (74,5%) assign IP addresses using Dynamic Host Control Protocol (DHCP), 15 respondents out of 55 use static IP addresses, and 14% don't know how addresses are assigned.

In terms of connection type, 28 respondents out of 55 (50.9%) have ADSL connections; 21 respondents out of 55 (38.2%) use optical fibre; 8 respondents out of 55 (14.5%) both for HDSL and wireless bridge;

1 (1.8%) answer for 3G/4G. Only 12.7% have a double connection (for instance, ADSL and wireless bridge).
Speed connection's question was divided in download and upload speed as shown by results in the Table 1.2

SPEED CONNECTION	Up to 2Mbps	from 2 up to 10Mbps	from 10 up to 50Mbps	from 50 up to 100Mbps	over 100Mbps
DOWNLOAD	5.4%	12.8%	12.8%	38.1%	30.9%
UPLOAD	12.8%	16.3%	20%	34.5%	16.4%

Table 1.2: Specify speed of the Internet connection

The final question on ICT infrastructure and services area was about how schools manage services such as a website, email, Domain Name System (DNS), Learning Management System (LMS) and online student records. Results are shown below in Table 1.3.

How do you manage following services?			
	Self-managed Server Inside School	Remotely (In the Cloud)	Not Available
WEBSITE	40%	58.1%	1.8%
MAIL	21.8%	76.3%	1.8%
DNS	40%	45.4%	14.5%
LMS	30.9%	36.3%	32.7%
ONLINE STUDENT RECORDS	29%	49.1%	21.8%

Table 1.3: How do you manage the following services?

2 ICT Security

2.1 Overview

The use of the Internet and Information and Communication Technologies (ICT) continues to increase across Europe. Young people have been among the first to take up the new technologies and services, and represent the largest user group of online and mobile technologies. In the EU, a much higher proportion of young people (aged 16-29) made use of a computer and the Internet on a daily basis than the rest of the population, with four out of every five (80%) young people using a computer on a daily basis in 2014, nearly 20 percentage points higher than the whole population (63%)[4]. Furthermore, the Net Children Go Mobile project study [5] suggested a shift towards a post-desktop media ecology when children (aged 9-16) used devices instead of a desktop PC to access the internet. Among all the devices: desktop (33%), laptop (46%), smartphone (41%) and tablet (23%), smartphones were used the most on a daily basis (41%).

For many years, governments, regions and schools across Europe have made significant investment in ICT connectivity, infrastructures and services, with the aim of making digital age teaching and learning a reality for young students, to equip them with the competences needed to meet the challenges of the 21st century.

Schools are using an increasing amount of networked information, and the principles of ’always-on’ education and bring your own device (BYOD) use mobile devices as an essential part of teaching and learning. The Organisation for Economic Co-operation and Development (OECD) document “Students, Computers and Learning: Making the Connection” [6] reports the amount of time within a typical school week that students spend using the Internet at school and at home, both during school days and on weekends. The document does not compute specific time (the answers were given on a categorical scale) students spend online, but it does estimate of “over two hours” each day across the OECD countries.

Internet and ICT open a huge range of possibilities for teenagers and children, widening their horizons, giving them unexpected opportunities to learn, create new and different identities and participate in society. In the same time, however, they can also be exposed to risks when online, such as giving out their private details, cyberbullying or grooming for sexual abuse.

Therefore, Internet and ICT use within a school environment deals not only with the tools pupils and teachers choose for their lessons, what learning management system or file-sharing system they decide to run, or if they browse the web with computers or just download data with smartphone apps. It also deals with multiple issues about ICT security, affecting the network, operating systems and applications. This is a very critical aspect and there is a strong need for schools and the higher education system to have a better understanding of the context: what kind of threats and weaknesses schools have to face, what kind of related countermeasures apply to protect network infrastructure and what are the basic policies schools can adopt to safeguard technological infrastructure and data.

2.2 Approach

EU Directive 2016/1148 [7], the Network and Information Security (NIS) Directive, points out the vital role that network and information systems and services play in society and clearly declares that their reliability and security are essential to economic and societal activities (art. 1). Article 2 of the same Directive raises an alert: "The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union".

The NIS Directive aims to bring cybersecurity capabilities to the same level of development in all the EU Member States and to make sure that they have minimum skills to ensure a high level of protection against Internet threats in their territory.

Despite these clear statements, digital security is a complex issue to approach and, for this reason, it is of the utmost importance to the UP2U project, addressed by several work packages. ICT environments are becoming more and more heterogeneous and complex and, as a consequence, are likely to be exposed to new type of intrusions. Whether this is a relevant problem to solve for huge organisations able to invest a significant part of their budget on cybersecurity, we can easily understand how this can be a tricky wall to climb for schools that constantly deal with budget constraints. In addition, considering the still high technological diversification and the different mastery levels of ICT tools within schools, this aspect deserves a deep level of attention and requires the need for additional effort to provide guidelines and means that can help schools to manage their security needs.

The main problem to solve is economic. As any other organisation, schools need to assess the cost-effectiveness of ICT security measures. But it is difficult for organisations to exactly measure these costs and their effectiveness, because security is an investment in loss prevention. What is the right amount a school should invest in protecting information? It depends on many factors but the proportionality of costs is the always valid parameter to take into account. In general, spending to ensure the required level of protection should be less than the cost to sustain for the recovery of damage as a result of an attack. In other words, taking into account the scarce resources available for schools' investment in ICT infrastructure, security budget should always be carefully sized, avoiding the use of technologies that are too much sophisticated, costly and hard to manage.

The following part of this section lists some basic notions and requirements on ICT security and then analyses the survey to check schools' situation.

2.3 Information Security

Information is a major component for the activity of each institution and, as a consequence, it must be adequately protected. ICT security aims to protect information against a wide range of potential attacks in order to ensure continuity of the activity, minimise damage and breaks in service.

Information security programs are based upon the main objectives of the CIA triad: maintaining the confidentiality, integrity and availability of IT systems and business data.

The CIA triad:

- Confidentiality: ensures information accessibility only to those who have permission. In other words, a set of rules that limits access or places restrictions on certain types of information.
- Integrity: guarantees the accuracy and completeness of information and processing methods. Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.
- Availability: ensures authorised user access to the information when needed.

Security requirements definition comes from:

- Risk assessment on an organisation's asset exposition, and the potential damages resulting from such exposure.
- Quantification and classification of the so-called “residual risk” (residual risk is the threat that remains after all efforts to identify and eliminate risk have been made).
- recognition of the set of legal, regulatory and contractual requirements to which the organisation and its suppliers must comply.

2.4 Security Policy

A security policy is a written document that sets formally how an organisation plans to protect its physical and information technology assets. This document is the starting point to reach any effective objective of ICT security, and thus represents an essential management support tool. There are a number key goals that should be sought by a security policy.

Main goals for technological resources:

- Service availability in a suitable mode, even when facing exceptional events, through the formulation of appropriate plans for recovering the system functionality.
- Continuity of service to cover an organisation's operating needs.

Main goals for data:

- Information confidentiality.
- Information integrity.
- Accuracy of critical information for any eventual consequence arising from their alteration.

- Availability of information and related applications.

Physical Security

Physical security is the protection of hardware, software, networks and data from physical actions and events that could cause serious loss or damage to the organization.
Main goals of physical security include:

- Protection of people.
- Physical and functional integrity of equipment.
- Avoiding unauthorised operation causing significant damage to the organisation or interacting people.

Bring Your Own Device (BYOD) in schools and the Internet of Things (IoT) for enterprises is widening the sphere of physical security as smart devices connected via the internet may be located outside of recognized secure perimeters. Isolating these smart devices can't be achieved in the same way as those within an organisation's physical borders. We'll see later on, what implications have BYOD and "always on" connections for school ICT security.

Logical security

Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation [8].
Main goals of logical security include:

- access control to IT resources to protect against intrusions, internal and external attacks.
- Security in storage and transmission.
- Service availability.
- Information availability to investigate potential violations.

2.5 Information Classification

Information classification is the basic activity for risk assessment and the potential damage that an incorrect use of information can generate. Classification should not be related only to computer data, but it must be extended to all types of information, documents and the software that handle them.

2.6 Risks

The risk of destruction or corruption of data due to an attack or some unexpected incident is the risk mostly addressed by ICT security policies. Risk assessment defines the probability of various types of incident with their predicted impacts or consequences. In this section, we quickly list some of the most widespread risks, categorised as external and internal.

External risks

- Unwanted access: accessing internal network from strangers or unauthorised persons, exposing workstations and data contained at risk of tampering or removal.
- Virus: Internet browsing and e-mail are the main vehicles for spreading viruses. Risks associated with virus infection are loss of data, unauthorized access, computer and devices blocking.
- e-mail spamming: receiving false and unsolicited e-mail traffic. If unmanaged, this risk can cause:
  - Blocked e-mail servers
  - An increase in network traffic and overload with slowdown of applications.
- Phishing for identity theft: Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise/organisation in an attempt to scam the user into surrendering private information that will be used for identity theft.
- Data interception and theft: transmitted data, before reaching their destination, are managed by different devices; data can be intercepted, modified, read or stolen with privacy and integrity violation.

Internal risks

- Illegal data transmission: confidential data can be illicitly transmitted to individuals not authorised to receive and manipulate such data.
- Browsing websites with offensive contents: web surfing should be subjected to filtering, avoiding access from internal network to inappropriate webpages.
- Traffic not allowed: free access to the Internet can interfere heavily with institutional activities. Download and exchange of apps, images, music and video files (through the so-called peer to peer mechanisms), if not regulated, overloads the network. To avoid this, traffic can be restricted, for example, to certain timeslots or, more effectively, by adopting automated partitioning and assigning necessary bandwidth to institutional activities thus preventing undue network use.
- Tampering, system damage, back-door opening: intentional malfunction or sabotage caused by either the normal users of a product, package, or system or others with physical access to it. Following changes in personnel, withdrawal of access rights and equipment is needed, if no longer necessary or allowed.

2.7 Denial of Service (DoS) and Distributed Denial of Service (DDoS)

Denial of Service (DoS) is a network attack that prevents legitimate use of server resources by flooding the server with requests. During DoS attack, the attacker overloads a site’s server with requests for access far above the capacity of the site, avoiding legitimate requests to be processed.
DoS attack can include:

- Disrupting service to a specific person or system, flooding a network with traffic to prevent legitimate traffic flow.

- Preventing a person from accessing a particular service and disrupting the connection between two specific machines, thereby interrupting a service.

Another type of DoS attack is the so-called e-mail bomb, wherein a large number of spam emails are sent in order to disable a mail server.

Distributed Denial of Service (DDoS) attacks are launched from multiple connected devices that are distributed across the Internet. DDoS is a type of DOS attack where several hacked systems are used to target a single system causing a DoS attack. DDoS attack victims are both the end targeted system and all systems maliciously controlled and used by the hacker. In a DDoS attack, the inbound traffic flooding the victim originates from many different sources, thousands or more, thus making it impossible to stop the attack simply by blocking a single IP address. Although DDoS attacks have always represented a challenging threat to internet systems, the propagation of botnets and the introduction of new attack vectors, together with the rapid adoption of broadband globally in recent years, have powered the effectiveness of such attacks.

In order to contain most intense attacks' effects, it is necessary to coordinate with the Internet Service Provider (ISP) providing network access. The ISP, aiming to protect other customers, could be forced to discard, on the border routers, victim's traffic. Of course, this effectively prevents access, even to legitimate users, but saves the network backbone and peering connections.

2.8 BYOD: Main Risks and Contradictions

Recent research reports that the range of online activities children and young people take up varies by age, following a progression from basic uses such as gaming and school related searches to creative and participatory uses of the internet, such as maintaining a blog, creating and sharing their own content [9]. The same research states that 35% of children (age 9-16) use the internet for schoolwork and that, among all the devices, smartphones are the ones that they are more likely to own (53%) or use to go online.

Schools in various countries are implementing BYOD because of its potential to deliver benefits to learning but this entails a range of challenges and risks associated with. Furthermore, BYOD policy is contradicting: some European governments are funding BYOD pilots or have a BYOD strategy, but schools in other European countries say there is not a clear national direction on how to proceed [10].

There are a number of considerations when reviewing the risks linked with smart device utilisation in schools. School-managed computers can be configured with security policies to avoid malicious infections and malicious systems, while BYOD devices are under the user control who does not only use them for education purposes but for any sort of activity, installing diverse kind of applications, thus implying a higher risk. Especially tablet and smartphone apps, though downloaded from trustworthy stores on the internet, do not warrant they have no malware infection.

It is advisable to enable malware detection systems to analyse internal traffic and isolate compromised systems. By vocation, schools' environment has to be as open as possible to foster collaboration, so it could be inappropriate adopting the same business environment security policies and technologies.

A first approach can be network segmentation and segregation, creating clear separation of data within the network, for example separating sensitive and administrative data on a protected network partition, from the one used by students. This model can be extended to multiple levels when it is possible to identify system groups with distinct operating environments (video surveillance, building automation systems, access control, timer, printers, Network Attached Storage, IoT, etc.).

Network monitoring systems to detect anomalies and abuses, rather than attempting to configure wider restrictions, could be a second step. This solution involves continuous monitoring and analysis tools to keep up with threats. At the same time, an identity management system must allow rapid detection of the source of threats.

The culture change of BYOD can be very difficult for technical support staff in schools and they may be reluctant to co-operate with BYOD plans, for several reasons:

- Pre-registration of all devices and IP addresses which are to be allowed access to school networks is a large task that only IT staff can undertake.

- If a school's BYOD strategy includes providing responsibility for supporting the students' devices, the number and knowledge of IT staff currently employed may be insufficient, necessitating additional investment in staff and staff training or outsourcing of ICT support[1].

2.8.1 Bring Your Own Device: An Example from the Greek School Network

Security issues that BYOD policy raises can be dealt with combined approaches. For example, the Greek School Network (GSN) provides central Lightweight Directory Access Protocol (LDAP) services for authentication. The teachers own accounts which are annually and automatically renewed. Moreover, they have the ability to create similar accounts for their students.

The Central User Authentication Service (https://sso.sch.gr) provides access to a member of GSN from a single point (Single Sign On) in all integrated applications of GSN and in authorised services of the Ministry and other educational partners without the need for re-accreditation of the user in each one of them. For GSN the safe access of students to the Internet and their protection against inappropriate content is a fundamental principle. Since 1999, GSN has operated a content control service on the web and applies a secure content policy, in line with the international best practice and legal requirements.

After connecting their device to the Greek School Network, the access of both teachers and students is filtered and therefore potential dangers hidden behind pages with offensive content are avoided. The Web Filtering Service cannot be bypassed by the users (transparent proxy).

This service denies access to websites that contain:

- Messages about hatred, violence and propaganda of aggressive behaviour.

[1] See [10].

- Messages to promote or use drugs.
- Gambling.
- Pornographic content;
- Racist messages or promotion of racism (hate speech).

Since 2013 GSN (CTI) participates as a national coordinator in eSafety Label action of the European Schoolnet. Through this action Greek schools can attain a special certification which aims to the support of schools in order to provide a safer online environment for teachers and students. Quantitative indicators of eSafety Label bring Greece in the first place in Europe [11].

2.9 Cloud and Virtualisation

According to EU Directive 2016/1148, Network and Information Security (NIS) Directive[2], “the term ‘cloud computing services’ covers services that allow access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services”. According to the directive, cloud computing services span a wide range of activities that can be delivered according to different models.

Virtualisation systems and technologies have revolutionized the traditional view of ICT and are permeating many ICT domains and fields of today’s society. Virtualisation is at the basis of cloud computing and networking, supporting better performance, transparency and portability and interoperability by combining hardware resources, software resources, and network functionality into a single, software-based administrative entity. Nevertheless, the price for such benefits is a negative effect on security of systems [12].

With regard to schools, cloud services and virtualisation can provide a radical increase in the efficiency and effectiveness of such organisations and communities, but this also bears a number of new security risks. “Some risks are shared with traditional computing environments and include, for instance, issues affecting operating systems, communication protocols, and applications, but these issues may even be exacerbated by the use of virtualized components, producing a greater security impact” [3].

The above mentioned Directive (Art. 54) asks public administrations, such as schools to apply additional security measures when adopting cloud services: “Where public administrations in Member States use services offered by digital service providers, in particular cloud computing services, they might wish to require from the providers of such services additional security measures beyond what digital service providers would normally offer in compliance with the requirements of this Directive. They should be able to do so by means of contractual obligations.”

The main concern for cloud services and virtualised systems, is about data protection and privacy, which needs to be strengthened in environments where multiple entities operate on the same infrastructure. Data must be protected, not only from access by unauthorised agents, but also from

[2] See [7].

[3] See[5]

the parties that perform processing and storage, which are not necessarily trusted. This cannot be achieved only with traditional cryptosystems and current security frameworks [13].

Despite the ongoing security issues, cloud services are a cheaper option for education in the face of funding cuts. If educational organisations currently store software and data locally, moving to the cloud will allow them to spread out IT costs through more flexible subscriptions. Such software as a service (or on-demand software) is a cheaper alternative to the large costs associated with the purchase of upfront licences [14].

A high number of universities and research centres have migrated much of their infrastructure to the cloud. Security is an especially pressing issue for these institutions that have found a way to meet such competing demands for greater agility, less risk and lower cost. Solutions aim to empower data owners to maintain control over their data, their distribution and sharing, thus providing verifiable and privacy-enhanced data management.

2.10 ICT Security: Findings and Considerations from Survey Analysis

This section of the survey investigated awareness of ICT infrastructure security and how schools manage some relevant issues about this topic. Before starting the analysis, a consideration is needed: in the majority of cases, the whole European education system deals with the problem of computer equipment aging in schools' labs. This is one of the biggest concerns to face to improve security systems and BYOD is not a solution, but rather a mean that can complicate things with regard to security, as we said before. Daily, new vulnerabilities are identified in applications and system software, thus allowing machines to be threatened or infected. Systems upgrading should be an automated mechanism, but when operating systems become obsolete, security updates are no longer released, thus making software exposed to attacks.

BYOD is even harder to manage: access to school services from students' devices increases the risk of compromising system security and, furthermore, while students use their devices at school with school provided and managed software, their personal data need to be protected. "For example, if the school remotely updates software on the students' device, personal data must not be lost. Managing secure access to school data and protecting students' personal data means an increased workload and responsibilities for school ICT support staff. IT departments supporting corporate BYOD, for example, are increasingly interested in the concept of, and tools that enable, 'containerisation', i.e. separating corporate data from employee data on employees' BYOD devices. Such tools are currently relatively expensive and generally schools are not considering these."[4]

The first question of this section was to investigate the perception that respondents have about security of their school's network. On a scale from 1 (Not at all) to 5 (Completely safe), most of the answers are between 4 (43.6%) and 5 (16.4%); 29% on 3 and 5.5% for both 2 and 1 (Figure 2.1).

[4] See [10]

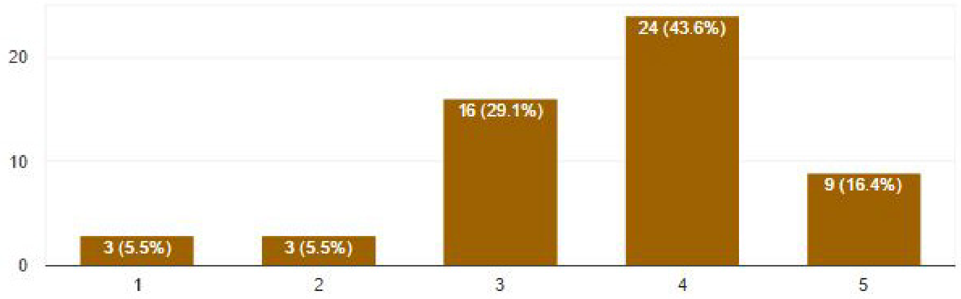

Figure 2.1:: How safe do you think your network is?

49.1% of respondents says school has a formal document (policy) about security and risk management for networking (36,4% of responses on “no” and 14,5% on “don’t know”) (Figure 2.2).

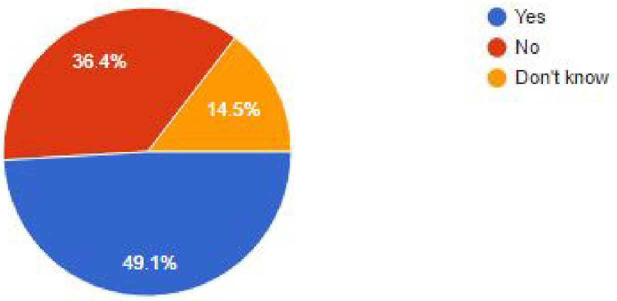

Figure 2.2: Does your school have a formal document (policy) about security and risk management for networking?

70.9% of the sample report that their schools do not have an IT security officer (23.6% answered “yes”) and the following open-ended question linked to this one (If you answered “yes” to the question above, please indicate his/her role) tells us that, actually, there are no specific persons in charge of it.

ICT security support relies on: periodic password changes (30 responses on 54 – 55.6%); training for users and administrators (24 responses on 54 – 44.4%); redundancy plans (Disaster Recovery) (19 responses on 54 – 35.2%). 11 on 54 (20,4%) say they do not provide any kind of support and 6 (11.1%) don’t know.

Access to the network is allowed to: 45.5% all users authenticated by password or other method; 25.5% only teachers, students and administrative staff; 16.4% all (internal and external) users anonymously; 12.6% only teachers and administrative staff (Figure 2.3).

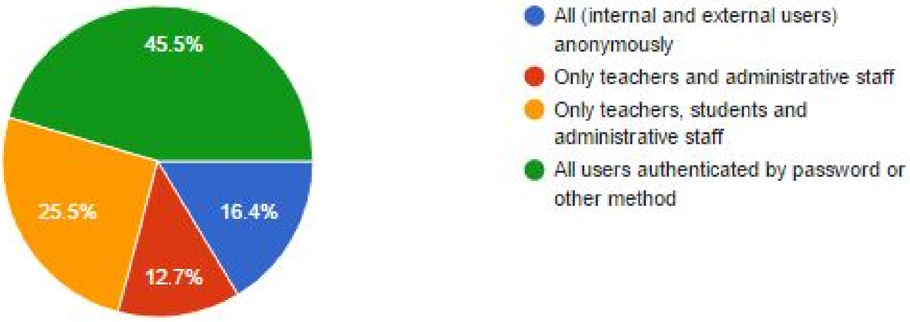

Figure 2.3 The following can access the network

A wide range of devices is connected to the network: schools' computers (55 responses on 55 – 100%); laptops/notebooks owned by teachers and/or administrative staff (52 responses on 55 – 95.4%); 44 responses on 55 (80%) both for server and mobile devices (smartphones, tablets, wearable) owned by teachers, students and administrative staff; interactive whiteboard (29 on 55 – 52.7%); security cameras and video surveillance systems (21 on 55 – 38.2%); only 1 (1,8%) answer for time tracking systems.

40% of respondents says their schools hold a formal document (policy) for network access (38.2% "no" and 21.8% "don't know") as shown in Figure 2.4.

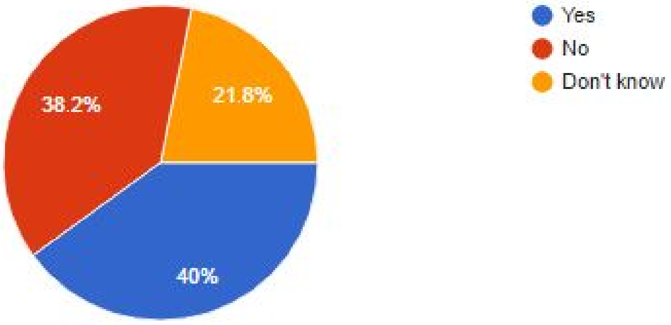

Figure 2.4: Does your school hold a formal document (policy) for network access?

A teacher and student authentication system for wired/wireless access to the network is provided in the schools of most of the respondents: 63.6% for wired access; 70.9% for wireless access.

Nearly half of the interviewed sample ignores what a DoS or DDoS attack is (Figure 2.5). This is a very important aspect to consider: as we said, DoS and DDoS attacks are one of the main threats for network. If schools' staff is unable to recognize this kind of threat, it is impossible to coordinate with the Internet Service Provider in order to contain most intense attacks' effects.

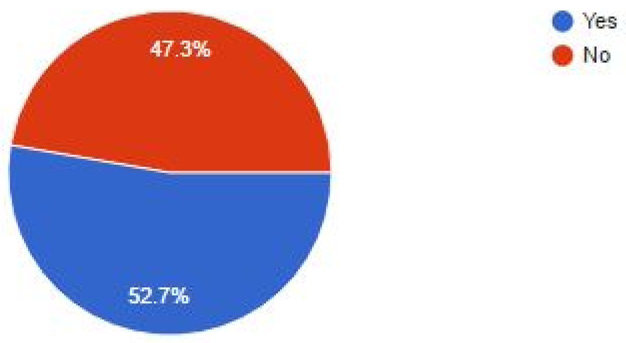

Figure 2.5:: One of the main threats for network is the DoS (Denial of Service) and DDoS (Distributed Denial of Service) attack, which can affect whole networks, Internet Service Providers or services. Do you know how these attacks take place?

Internal ICT security rules (Figure 2.6) are included in a formal document in 30.9% of cases (38.2% answered "no", 30.9% "don't know") and cover computers (50 responses out of 55 – 90.9%); network connections (38 responses out of 55 – 69.1%); software (36 responses out of 55 – 65.5%); data (23 responses out of 55 – 41.8%).

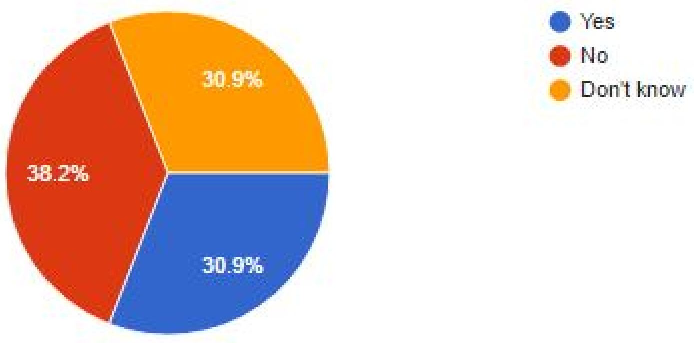

Figure 2.6:: Are the internal ICT security rules included in a formal document?

67.3% of respondents are aware that their network can be exposed to internal and external risks (Figure 2.7) and the most of them, asked to list any of these risks in the following open-ended question, reported virus, malware, and data theft. Only 5 out of 23 (21.7%) mentioned DoS attacks.

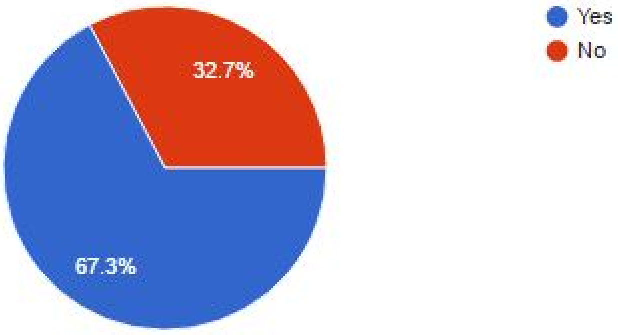

Figure 2.7:: Are you aware that the network may be subject to internal and external risks?

3 Data Protection and Privacy

3.1 New European General Data Protection Legislation

Introduced by the General Data Protection Regulation - Regulation (EU) 2016/679.

First review of legislation, with particular attention to the applicable rules to a "*cloud-based digital learning infrastructure*" and the most relevant implications for schools and other subjects that treat the personal data of children.

The following section intends to provide an overview of the new European Privacy Policy. This version would like to offer a first look at the discipline and its fundamental principles. The text was written specifically considering the occasions when minors are coming into contact with the "*Information Society*" offering services. It is recommended that you keep a copy of the Regulation, available in all European languages at the following link: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679.

RECITALS:

- The European Regulation 2016/679 (hereinafter referred to as "the Regulation" or "GDPR") was adopted on 27 April 2016.
- The GDPR updates privacy legislation and disciplines in a very detailed manner how personal data is processed.
- The GDPR has been adopted by regulation and therefore does not require any form of application law by Member States.
- The rules contained in the GDPR will become effective and binding from 25 May 2018, after a transition period of two years.
- The Up2U Project has among its objectives to propose a "training" course that has as its target audience, in large majority, subjects not yet aged.
- The UP2U Project is geared towards the development of a cloud-based, economically viable and e-Learning platform (Challenge 1: Develop and test open, interoperable components for a flexible, scalable and cost-effective cloud-based digital learning infrastructure).

SO:

- It is appropriate to examine the Regulation by highlighting the practical implications of the rules on the retention and processing of personal data, particularly where minors are involved.

Children, in fact, need specific protection of their personal data as they may be less aware of the risks, consequences, safeguard measures and their rights in relation to the processing of personal data.

This concerns, in particular, the use of personal data of minors for marketing purposes or the creation of personality or user profiles (cd profiling) and the collection of data concerning the child when using services directly provided to a child minor.

European Regulation 679/2016 (GDPR), pays special attention to personal data processing for minors by invoking specific safeguards and protections.

Especially teenagers, large web and social network users, are often unaware of the risks associated with sharing their personal information, ignore their rights and do not care that the information they have about has been acquired and then kept in accordance with security principles and correctness.

It is important to remember that from May 2018, the Regulation will be the common regulatory fabric for European privacy laws. The GDPR has been adopted by the Regulation and therefore does not require any form of application law from the member states.[5] This implies that the same identical legislation will apply in all Member States, but that is not the case. There are two exceptions, the first concerns the minimum age for the validation of consent to the processing of data, the second concerns the subject of professional secrecy. In the following, we will deepen the issue of valid consent by minors, while professional secrecy is not currently the subject of our interest.

To begin with, a brief overview of the important novelties introduced by this new regulation should be made.

3.2 Main News Introduced by the EU Regulation on Privacy

BREACH NOTIFICATION - ART. 33 E 34 GDPR:

It becomes compulsory, in any case where there is a breach of computer security, to immediately notify the fact (within 72 hours if there is a risk to the rights or freedoms of natural persons) to the Supervisory Authority provided for by the art. 55 GDPR and also to the person concerned.

33. 1. *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

[5] However, some provisions seem to leave a margin of discretion to individual EU Member States, I refer in particular to the minimum age requested for the valid consent to data processing (Article 8, paragraph 1, last paragraph, GDPR: "Member States may lay down a statutory minimum age for such purposes, provided that they are not less than 13 years old."). There is another hypothesis where Regulation Can be applied in a different way by the Member States, it deals with professional secrecy rules, which do not concern us here.

34. 1. *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*

RIGHT TO ACCESS - ART. 15 GDPR:

It introduces the right of the data subject to obtain from the data controller the confirmation that a personal data processing is in progress or not, and in the first case, to gain access to personal data and information such as: data-processing, data recipients, data processing duration, source of data (if not provided by the data subject). In addition, the data processor shall provide, upon request, a copy (free of charge and in electronic form) of the personal data being processed.

RIGHT TO ERASURE ('right to be forgotten') - ART. 17 GDPR[6]:

Also known as the "Right to Erasure" is the right to obtain the removal of your personal data, to stop the (further) dissemination of data and to stop the potential processing of data by a third party. The cancellation conditions, as described in Article 17 of the GDPR, relate to data that are no longer relevant to the original purpose for which they had been granted, because they were changed because the person concerned withdrew their consent to the treatment when the processing of data is not in accordance with the regulation in question. The subject responsible for data processing will have to reconcile different needs by comparing, at these requests, the “rights of subjects” with "public interest in data availability".

DATA PORTABILITY - ART. 20 GDPR:

The GDPR introduces the portability of data - which consists in the subject's right to receive the data concerning him (provided that they have been collected by means of electronic forms) and to transmit them to another Responsible for treatment.

PRIVACY BY DESIGN - ART. 25 GDPR:

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as “pseudonymisation”, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure

[6] See below: Whereas 63 - GDPR ART.16 – RIGHT TO RECTIFICATION AND ART.17 - RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN).

that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

The Data Controller is required to conduct a preliminary investigation of the extent of the risk of treatment and possible breach of the confidentiality of the information, including the nature of the information provided. Appropriate technical and organizational measures must be taken, limiting the availability of the data subject to processing to those strictly necessary for the purpose (minimization) or by taking appropriate measures to prevent the association of the data subject to treatment to the person (e.g. "pseudonymisation"). There is also a data protection certification tool (see Article 42).

3.3 Basics

GDPR Art. 4 Definitions

For the purposes of this Regulation:

A) **"PERSONAL DATA"** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The notion of personal data, therefore, concerns not only the person's distinctive data, but each one that, once associated with the person, allows identification.

Recently, just in Europe, the nature of "*personal data*" has been acknowledged at I.P. Address.

Personal data distinguish "*sensitive data*", which is personal data whose incorrect treatment or spreading poses a greater risk of injury to the rights and freedoms of individuals.

"Sensitive data" are considered personal data to reveal: racial or ethnic origin, religious beliefs, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political nature or trade union, or to reveal the state of health and sex life.

B) **"CONSENT":**

GDPR Art. 4 - *Definitions:*

11. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

The processing of personal data is permitted, subject to the consent of the person concerned.

Consent of the minor of 18 years: GDPR Art. 8 - *Conditions applicable to child's consent in relation to information society services:* with the explicit reference to the provision of services by the "*Information Society*"[7], for the purpose of authorizing the processing of personal data, the consent of the minor is considered valid, provided that he has reached at least 16 years.[8]

If the child is under the age of 16 (but older than 13 years), where the individual State has applied the derogation in its legal order[9], the treatment is only permissible if and to the extent that such consent is granted or authorized by the holder of parental responsibility.

Therefore, it is important to emphasize that the consent of the major of sixteen years is valid without any further authorization. However, for children under the age of 16 (and upper than 13), the consent or authorization of the one who has the parental responsibility is required.

The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology (Art. 8).

The reference to "*available technology*" reminds us that we are moving in the context of relationships held by the child when receiving the services, by the "information society". But above all, it makes the declaration of parents authorisation, (sent by telematics means) sufficient to be considered authorized by the parent. The wording of the rule: "*taking into consideration available technology* " is peacefully interpreted as excluding the liability of the data controller in the event of false statements made by the child.

WHEN THE CONSENT IS REQUIRED:

Art. 6 GDPR:

[7] Article. 4 co. 25 of the GDPR defines: “*information society service* means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council.” In summary, "*information society service*" can be defined as any service normally provided for remuneration, remotely, electronically and at the individual request of a recipient physical service provider.

[8] Article 8: *“Conditions applicable to child's consent in relation to information society services 1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. 3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.
3. ... omissis.”

[9] Article 8.1. last part: *“Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.”*

Consent is required when the processing of personal data has one or more specific purposes[10].

There are some exceptions. In these cases, consent is not required, although personal data are treated for specific purposes, let's see:

WHEN THE CONSENT IS NOT REQUIRED:

The consent of the person concerned is not required (even where the treatment has one or more specific purposes) in a series of hypotheses, which the European legislator has foreseen:

Art. 6 GDPR:

(b) processing is necessary ***for the performance of a contract*** *to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

(c) processing is necessary ***for compliance with a legal obligation*** *to which the controller is subject;*

(d) processing is necessary ***in order to protect the vital interests*** *of the data subject or of another natural person;*

(e) processing is necessary ***for the performance of a task carried out in the public interest*** *or in the exercise of official authority vested in the controller;*

(f) processing is necessary ***for the purposes of the legitimate interests pursued by the controller*** *or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Public school institutions may only deal with personal data necessary for the pursuit of specific institutional goals or those explicitly provided by sectorial legislation. For such treatments, they are not required to ask students consent (GDPR - Art. 6 lett. e: *public interest task*).

Schools, however, often treat certain categories of personal information of students, not only students but also family members, relatives, cohabiting people, etc.

During the annual enrolment of the child to the school and during the provision of the school services, personal data of the minor, or data of parents or who has the responsibility of the child (such as healthiness, telephone, telematics and other data necessary for 'Provision of services such as: canteen, transport, sporting activities or participation in courses or school trips) are collected by the school.

[10] Processing shall be lawful only if and to the extent that at least one of the following applies: (*a) "the data subject has given consent to the processing of his or her personal data for one or more specific purposes".*

Some of these data may be “sensitive” or judicial data - As we have seen, when schools access "further" data, which is beyond what is strictly necessary to provide the services provided, “consent” is needed. It is also necessary that there be a "Data Controller". Anyway the school must verify the relevance and completeness of the data, but also their indispensability over the purposes it intends to pursue.

FORMS OF A VALID CONSENSUS MANIFESTATION:

Consent should be expressed through an unambiguous positive act by which the party concerned expresses the free, specific, informed and unambiguous intention of accepting the processing of personal data concerning him, for example by means of written declarations, also of electronic means, or oral. This may include selecting a box on a website (not to be pre-selected by the service provider), choosing technical settings for information society services, or any other statement or other behaviour that clearly states in that Context that the person concerned accepts the proposed treatment. (30)

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

Art. 7 GDPR - *Conditions for consent*

1.Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2.If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

The consent must be explicit, informed and the information regarding the treatment and its purpose must be clear. Consent is also revocable.

FORMS OF A NOT VALID CONSENSUS MANIFESTATION:

It is not a valid expression of consent to the processing of data: silence, inactivity or preselection of boxes.

Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.[11].

If the processing of personal data requires the consent of a minor under the age of 16, regarding the provision of services by the "Information Society", the Data Controller shall seek to verify that the

[11] Whereas 32 - GRDP.

consent is expressed or authorized by the holder of parental responsibility on the child using the technologies available[12].

AGE REQUESTED FOR VALID EXPRESSION OF CONSENT:

The minimum age for the valid expression of consent is generally the age of majority, which is recognized in the EU member states at the age of 18. As we have already seen above, the general rule provides for an exception only in relation to the provision of services by the "Information Society". Some European states already apply the 13-year limit, even for assent to "profiling.[13]"

WITHDRAWAL OF CONSENT: the Regulation provides that the revocation of the consent must be as simple as it is to give the consent (Art. 7 co. 3 GDPR: "*The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent*").

C) "DATA CONTROLLER AND DATA PROCESSOR":

Whereas 74 - ARTT. 24, 26, 27, 28 E 29 GDPR EU

Art. 4 Definitions (…follows): **"DATA CONTROLLER"**

Co. 7) *'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

Art. 4 Definitions (…follows): **"DATA PROCESSOR"**

Co. 8) *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

The Data Controller and the Data Processor are not necessarily mandatory figures within each structure. In general, these figures are required in cases where public bodies or businesses tend to have regular and constant personal data processing. As we have seen, when schools access "further" data, which is beyond what is strictly necessary to provide the services provided, "consent" is needed. It is also necessary that there be a "Data Controller".

The DPO (Data Protection Officer) - Art. 37 n.5, 6, 7:

- Shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and has to be able to fulfil the tasks referred to in Article 39.

[12] This sentence excludes the responsibility of the ICT service provider in the event of false statements made by the child.

[13] "Profiling"*: means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; (Art. 4 n.4 GDPR).*

- May be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
- Shall publish the contact details of the data protection officer and communicate them to the supervisory authority.
- Must be equipped with adequate resources to carry out its tasks and maintain its knowledge.
- Must be able to communicate directly with hierarchically higher management within the body.
- Does not perform other activities that could cause a conflict of interest.

Whereas 74

The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established.

In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

3.4 Rules of GDPR: Directly or Indirect Child Protection

Whereas 58 - Art. 7 CO. 2 – Art. 12 - GDPR - CLEARNESS:

The information intended for the public or the data subject must be: concise, easily accessible and easy to understand, with simple and clear language, as well as, where appropriate, visualization.

This provision meets the specific needs of children, who need special protection when the treatment concerns them. Any information about it and above all, any communication should use a simple and clear language that a minor can easily understand.

Whereas 59 – Art. 7 e 12 GDPR – Data subject rights: ACCESS, RECTIFICATION, DELETION, OPPOSITION:

It is appropriate for any person that process personal data, to provide for ways to facilitate the data subject exercise of the rights provided for in the Regulations. In particular, the right of the data subject to apply for and, where appropriate, to obtain (free of charge): access to data, their rectification and deletion, or to exercise the right of opposition.

We remind that the data controller will have to respond to the requests of the data subject at the latest within a month or will still have to justify the denial. There is no *non-response.*

Whereas 60 – Art. 13 GDPR – OBLIGATION TO INFORM:

THE DATA SUBJECT MUST BE INFORMED ABOUT:

1. The existence of the treatment and its purposes.

2. The existence of a profile and its consequences.
3. Any other information relevant to the specific case.

Whereas 61 – Art. 13 e 14 GDPR – … OBLIGATION TO INFORM: “when”

Whereas 62 - Art. 13 e 14 GDPR – - OBLIGATION TO INFORM: – exclusions

Whereas 63 - ART. 15 GDPR - RIGHT OF ACCESS BY THE DATA SUBJECT

Whereas 65 - GDPR ART.16 – RIGHT TO RECTIFICATION AND ART.17 - RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN):

RIGHT TO RECTIFICATION: the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

RIGHT TO ERASURE: Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

A natural person should have the right to rectify personal data concerning him and to obtain the deletion and termination of their dissemination if:

1. The data no longer serve the purposes for which they were conferred.
2. The consent was subsequently revoked.
3. The retention of such data does not comply with the GDPR or the law of the Union or of the Member States to whom the data subject is subject.
4. The data subject is opposed to the processing of personal data pursuant to the article and there are no legitimate reasons for processing.

This right becomes particularly relevant if the person concerned has given his/her consent when he/she was younger and therefore not fully aware of the risks arising from the treatment, and then wishes to eliminate this type of personal data, particularly from the Internet.

The person concerned should be able to exercise that right independently of the fact that he is no longer a minor.

However, further data retention should be lawful if it is necessary to exercise the right to freedom of expression and information, to fulfil a legal obligation, to perform a public interest task or in the exercise of public authority to which it is invested the controller for reasons of public interest in the public health sector for the purpose of archiving in the public interest, for the purpose of scientific and historical research or statistical purposes or to ascertain, exercise or defend a judicial right.

In order to strengthen the "*right to erasure*" in the on-line environment, the right should be extended in such a way as to oblige the person in charge of processing who has published personal data to inform those responsible for the processing that are processing such data to delete any link to such personal data or copy or reproduction of such data.

In order to ensure the above information, the data controller should take reasonable measures, taking into account available technology and the means at his disposal, also of a technical nature, in order to inform those DPO, who are processing the data, about the request of the data subject.

Whereas 71 – Art. 22 GDPR - AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING

Whereas 75 – Art. 32 GDPR

Whereas 75 and 76 – Art. A 25 GDPR – PRIVACY BY DESIGN

3.5 Data Protection and Privacy Awareness: Findings from Survey Analysis

This section focuses on the analysis of the new GDPR in force since May 2018, and questionnaires were designed to analyse the knowledge of the themes contained in them by the schools. The construction of applications, deliberately closed, provides a more comprehensive picture of institute awareness on the subject of privacy in order to build up future awareness and training actions. The first is that 70.9% of the sample does not know that starting from 2018, it will be mandatory to inform the Privacy Authority of computer security violations that accidentally or unlawfully entails destruction, loss, modification, unauthorised disclosure or access to personal data transmitted, stored or otherwise treated.

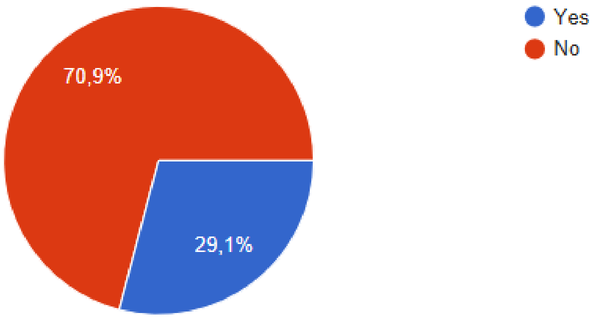

Figure 3.1: Do you know that starting from 2018 it will be mandatory to inform Privacy Authority of computer security violations that accidentally or unlawfully entails the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise treated?

The second question, “Did you know that the right to be forgotten aims to limit the dissemination of information to the person to whom they relate?”, had the following result:

- No: 50.9%
- Yes: 49.1%

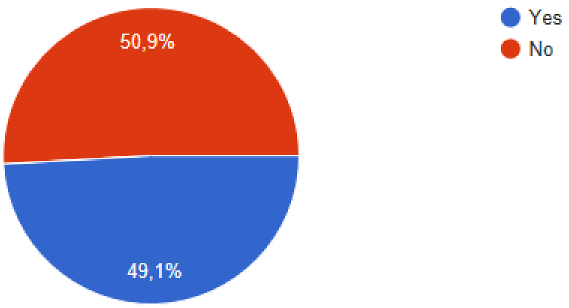

Figure 3.2: Did you know that the “right to be forgotten” aims to limit the dissemination of information to the person to whom they relate?

And again, the questions state that among the respondents:

- 65.5% do not know the meaning of the term pseudonymisation.
- 54.8% do not know that you can ask for the deletion of your personal data collected by subjects with whom you no longer have any relationships.
- 78.2% have never requested the deletion of your personal information.
- 90.9% do not know if their school has ever been asked to cancel their personal data.

With regard to some specific GDPR introductions, the following results are reported:

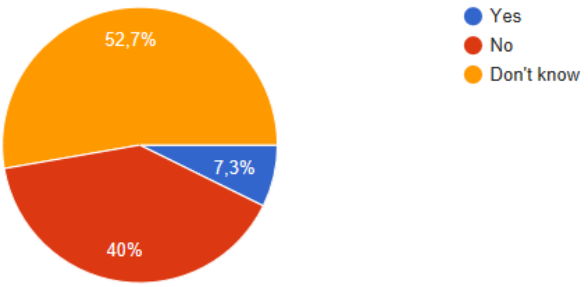

Figure 3.3: Does your school have a "Data Processor”?

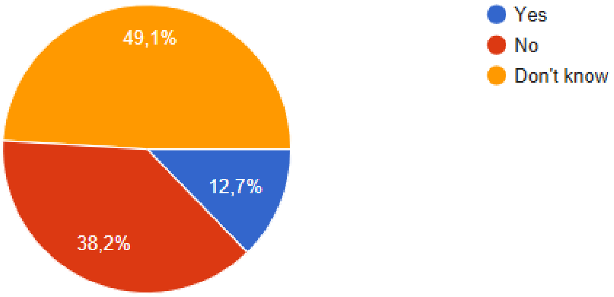

Figure 3.4: Does your school have a "Data Processing Controller" figure?

The last part of the privacy questions wanted to investigate the perception of schools on their ability to handle privacy and actions in place. The results were as follows:

- 60% do not feel that adequate protection measures are being taken to effectively limit the risk of identity theft or other forms of abuse.
- 70.9% declare that the school does not keep personal / sensitive information of minors on electronic media.
- 63.6% responded that they did not or did not know that on the occasion of data delivery by a minor under 16, the school did not request the consent of the child for data processing.
- 81.8% do not know if personal data collected is accessible from a terminal that uses an operating system or other application authorized to access system resources such as memory, image / video gallery, camera, microphone, position.

4 Identity Management

4.1 Main Problems and Behavioural Trends

The limits and the difficulties in establishing a regulatory framework for a pan-European electronic identity (eID) have been investigated by several studies.

The focus of EU-funded research projects and reports prepared for the European Commission in the eID and eGovernment sectors has been put to the legitimate obstacles to a pan-European eID system.

There is, in fact, a profound relationship between legal and technical aspects for eID Europe: although technology exists, legal interoperability lacks territorial dislocation of services based on electronic identity.

This analysis is much more useful in relation to the reference target of the Up2U project or 11 to 19-year-olds. Native digital, grown up in information and communication technologies that can reveal patterns, attitudes and behaviours about profiling, disseminating and protecting personal data.

The aim of this brief analysis on the issue of Identity Management is to outline the behavioural tendencies of students in European countries involved in Up2U in order to identify what standards can protect their identity without restricting their freedom of information and learning.

The issue of Identity Management is of great political and academic interest because the play of democracy, active participation and the right to individual growth is played on its territory.

The most frequently asked questions about the subject do not only concern the possibility and the way of authentication, but the responsibility for it as much as the Identity Management brings along a whole series of variables to control:

- Unreliable registrations
- Anonymity and pseudonymity
- Data Properties
- Security
- Responsibility

This section is dedicated to identity management. The following analysis of results also describes our approach to managing the identity of children in relation to their specific behaviour when using new technologies. This description takes into account the main trends in the behaviour of minors in the use of new technologies and the related problems (ID management and sensitization, identity theft, etc.)

The concept of digital natives, used for the first time in literature by Marc Prensky, defines the generation of students born and raised in the world of Information and Communication Technologies (ICT). This generation, according to the author, is native to the digital language of computers and the internet, thinks and processes information altogether differently to those who did not grow up with similar access to technology.

Digital Native Literature is conspicuous and initiatives that want to "understand" young people who grew up in the digital age are many. For this reason, this analysis comes from examining studies of nature, behavioural trends, and technologies used by digital natives.

These studies discuss whether digital natives, through their exposure to new technologies, have been cognitively altered by technology use and acquired advanced skillsets. Frequently asked questions in digital studies can be summarised as follows:

- Do digital natives think differently and learn differently?
- Do you become digital natives?
- What is the role of technology in defining the social behaviours of children between the ages of 11 and 19?
- Are digital natives really a technological generation?

Although there are different views on the characteristics of digital natives, there are some features on which all studies converge and are related to the quantity and quality of their technology uses. Conscious of this, in this section of the document, we intend to stimulate further debate on the issue of identity management. [15]

4.2 New Generations, New Technologies and New Privacy Perceptions

Literature on this topic describes us as digital young people as young enough disinterested in security and privacy issues; can we be content with this statement?

To better analyse the phenomenon, we report some data emerging from the EB 359 survey[2] that analysed the attitude of European citizens towards personal identity with reference to the use of social networks.

According to the survey, 34% of European citizens access Social Network, and 57% share video, images, music, etc.

Paradoxically, however, users who access the social network seem less cautious than non-social network users to share information on the Internet.

It is therefore possible to trace some of the characteristics of young people aged 11 to 19 in relation to Identity Management: they perceive their digital identity as a part of their identity and seem to decide who to give information and in what context they do not have a strong awareness of their privacy that they manage superficially. Too often, they are attracted to some advantage (for example, a discount) and do not care about sharing personal information, in summary, without wanting to, negotiate their privacy.

There is a clear need to equip people with the right tools to actively manage their privacy.

4.3 Challenges In Adopting Software as a Service in School

The school world is immersed in a process of user transformation and faces problems related to identity management [16]. Many of the tools in use in schools today are platforms provisioned via Software as a Service (SaaS), namely they live outside the perimeter of the school, within Google Drive, GoogleApps, Office365, the digital school record book, e-books, and the school website. Moodle is also an example of a service hosted outside the school.

To access all these SaaS tools, each student and teacher will need a digital identity, namely a username and password for each one of the services they need to access. The school institutions wanting to promote and effectively use digital technologies, not limited to the BYOD, but also by means of computer labs or institutional workstations, must prepare to manage and control their members' access to all the services they use, both inside the school and SaaS. For services provisioned by the school, the user is no longer using different digital identities created for each service, while the school takes care of managing digital identities, one for each of its members, performing operations of creating and assigning them to the users, monitoring their usage, updating and finally disabling them at the end of their life. The effort devoted to the digital identities management is rewarded with control and security provisioned to the users. It is not acceptable to waste the efforts of identity management by scattering it on all the SaaS platforms that the school decides to use.

The model of centralized identity management has begun to spread in Italian universities during the last ten years and is now fully operational, schools can count on a consolidated working model to follow.

4.4 Federated Identity Management: An Effective Tool for Managing the Digital School

One of the indicators for the evaluation of the proposals called in the Ministry of Education tender is having opted in to federated identity management. "With federated identity management we mean access to many resources and services through the release of unique credentials. This system makes the user's online activities easier and more secure, while at the same time reducing the credential management overload for those in charge of services, and eliminating the need to replicate credentials in a number of databases." It becomes then necessary to have tools and technologies to centralize the identity management, to improve management efforts and simplify the operations the user need to do. In the identity federation management model the SaaS administrator no longer has to manage user authentication, a complex and burdensome issue for the service, which does not provide added value, but only adds security problems and takes away resources and efficiency to the main business. Removing this burden, the services increase in security and efficiency. On the other hand, the school has to implement a new centralised system for managing identities.

By centralising identity management, the school can guarantee greater security to digital identities, add additional control features, such as a second factor of authentication, and provide users with tools to enforce privacy, all with greater efficiency. In this way the school can offer many services to teachers, staff, students and their parents. The advantage for the user is obvious: a unique password for accessing all online resources. With one password to remember we gain greater ease of use accessing multiple resources and a greater security having just one password to protect, while privacy is guaranteed because it is under control of the school identity management operator, who is the data controller of personal data of students, parents and teachers.

The communication protocol between federated identities and online services is Simple Assertion Markup Language (SAML). SAML decouples the user authentication from the access to a resource. The identity management and authentication are executed by a component called Identity Provider (IdP) located at the school, while access control (authorization) to the resource is done by a component called the Service Provider (SP). The SP, in order to decide if the user can log in, evaluates the assertion sent by the IdP to the SP. The IdP is the sole online service that receives the user's credentials. Each other service, whether internal to the school, or in the cloud, receives only the SAML assertion assumed necessary to decide whether the user can access or not.

The benefits introduced with federated identity management are:

- For the user: the Single Sign On (SSO) in accessing many services both internal and external to the organisation;
- For the school: a unified identity management, to enable control of who does what. All users who bring their laptops or devices at school (BYOD), while they access online resources, will be under control of the IdP, a system managed by the school.

Clearly, organisations that do not have implemented their own IdP, entrust privacy and users' monitoring to external services. A third benefit is for the resource provider, for which the management of its application is simplified.

4.5 Privacy in the Digital School[14]

Schools must take the responsibility of the personal data protection of people working, studying, or anything relevant to school activity. The Italian Privacy Act (Italian Legislative Decree no. 196/2003) establishes the "data minimisation principle: information systems and programs are configured to minimise the use of personal and identification data, so as to exclude the processing if the purposes sought in the individual cases can be achieved by using either anonymous data or mechanisms that allow identification of the individual only in case of need." SAML has the technological tools to enforce the provisions of the Privacy Act, and the school can transfer to providers only those personal data that are strictly necessary to provide the requested service. This means freeing the user from providing data in excess, avoiding to accept a treatment too invasive of privacy.

The IdP handles all the personal data of users (teachers, students, parents), organising them into homogeneous profiles in order to create and manage digital identities. The IdP, within its capabilities, can appropriately create the assertions intended for each service so that each assertion, directed to a specific service is built for each specific user, and contains only the strictly necessary information in order to allow the access and deliver the service. Each assertion is encrypted and signed to ensure confidentiality, integrity and non-repudiation during online transmission stages and reception by the recipient.

4.6 One Identity Federation for Universities and Schools and the Available Services[15]

Similar to the work undertaken for universities and research institutions during the last seven years by the IDEM Federation[2](coordinated and managed by the Consortium GARR[3]) an identity federation for schools could help improve security management.

The identity federation aims to ensure confidence among the participating organisations: the organisations, registering their Identity Provider and Service Provider in the federation, certify that the systems are under their control and responsibility. In the federation, communication between participants can only happen if the trust is maintained and actors communicate through encrypted and certified statements. In this way the transit online of personal data and digital identities is certified. At present, the IDEM Federation counts over 70 identity providers in Italy, delivering to date about 4

[14] See [14]

[15] Idem

million digital identities to students, researchers, faculties, staff and alumni of Italian universities. These end users can now gain access to about 1000 protected resources available in the world.

Already available in the IDEM Federation are some services useful to SAML-enabled schools: WiFi access throughout the national territory, videoconferencing GARR Vconf, mega-file sharing with Filesender, Le@rning-GARR, Terena Certificate Service, EduOpen, Dreamspark, Knodium. Other services are immediately configurable: for example any Moodle service, Wiki and CMS on various platforms, Google Apps, Office365, Box, Media Library On Line, Sebina Open Library, social learning platforms. Other services such as e-books and school record book platforms could be available if there was a critical mass making the request, as shown by the successful use case related to publishers in the US and Britain.

4.7 ID Management and Awareness: Survey Findings

Concise description of an identity management project in schools has been used to outline an attention scenario for certain secure management processes of identity.

This is a precondition for developing a new learning ecosystem as well as thought in Up2U.

Part of the Up2U survey deals specifically with identity management In order to investigate the attitude and the identity management actions carried out by the schools of the countries involved in the project.

The respondent sample, as analysed in the previous sections of the document, while not being statistically exhaustive of the situation helps to trace teacher and student behavioural trends in the use of ITC and some related themes. It also reflects example issues/solutions to recurring problems on identity management, including:

- 58.2% of respondents state that their school has an office or a person in charge of accrediting users.
- 52.7% of them indicate the presence of a personal identification document.
- Almost all respondents (99.51%) describe a method of delivering common and shared credentials within the school (such as by hand or voice delivery from the office or person in charge; by email from the office or person in charge; sent to users by post in a sealed envelope.)

These statistical results attend to the issue of identity management that has been further investigated with questions about the presence or otherwise of specifically dedicated staff and/or written policies such as unique rules for all school users.

From the answers obtained from the survey, just under half of the respondents state that their school has no policy and/or formal document describing the steps to be taken for users identification. The data is not extremely encouraging but well agrees with the tendency not to handle identity systematically. A number of questions and range of responses follows.

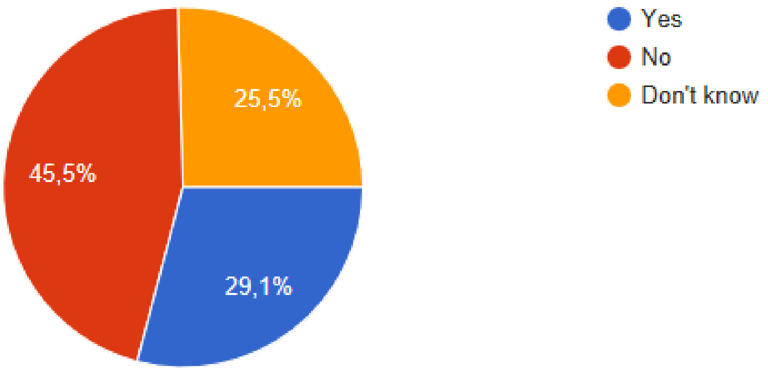

Figure 4.1: Do you have a policy and/or a formal document describing the steps to be taken for users identification?

Apparently counterproductive, nearly 50% of respondents say that their school provides users with instructions on their responsibility for custody and retention of confidentiality of access credentials. The data, on the other hand, tells us about a school that implicitly has rules of identity management that, most probably, did not express itself in a formally documented and formally approved form.

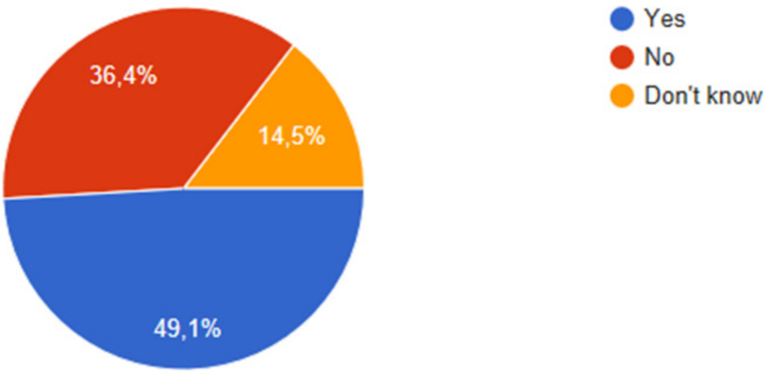

Figure 4.2: Do you have a policy and/or a formal document describing the steps to be taken for users identification?

Confirming a widespread lack of attention to identity management, the answer to the question: Is there a policy for managing credentials of Internet access?

29 respondents answer no (little more than 50%) and the answers of the remaining 26 are divided as follows:

- Yes, it is posted on the web (8 people).
- Yes, it is provided to users simultaneously with accreditation (8 people).
- Yes, but not published (12 people).

The questions submitted to the sample also sought to analyse the phenomenon of identity management in its entirety: from registering / authenticating the user to removing her credentials when she completed school relationships.

In this regard, we first asked when the user's login credentials are disabled, and the responses obtained included:

- At the end of the study / working relationship with the school (31 of 55 replies).
- After a few months from the end of the course (7 out of 55 replies).
- After an explicit renunciation for a student (7 out of 55 replies).
- After an implicit withdrawal, the student stops attending school (10 out of 55 replies).
- Never (10 out of 55 replies).
- After some time of inactivity or report from Google about breach (1 out of 55 responses).

Knowing when schools disable access to network credentials has helped us outline the level of awareness about whether or not to retain more or less sensitive data within them. In addition, we asked if the schools interviewed alert users when their credentials are expiring or disabled. The data serves to analyse how important the management of identity in individual schools is. The figure does not reflect behavioural peaks, though just over one third of respondents state that the school does not inform users.

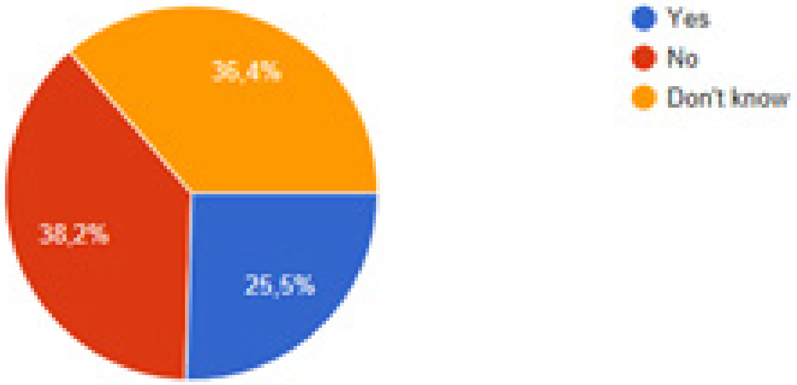

Figure 4.3: Does the school notify the user of account expiration/disablement?

If we wanted to get into a slightly more thorough analysis, we asked the schools whether they would permanently or completely dislodge users from their accreditation system. The following answers were given:

- 38.2% Yes, automatically after his/her deactivation/disabling.
- 43.6% Yes, occasionally and manually by an office/person in charge after his/her deactivation/disabling.
- 14.5% The user is never deleted.
- 1.8% No.
- 1.8% No credentials are available.

From the analysis conducted there is a split in identity management, especially in the presence of a transfer of personal data to a specific service provider. Just over half of the respondents say that they do not inform users of this passage, while the rest of them respond affirmatively, as shown in the following graph:

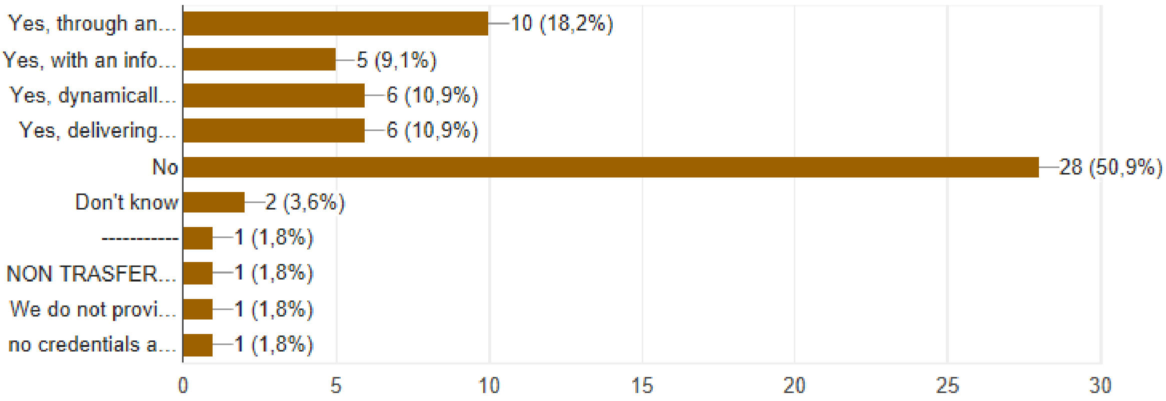

Figure 4.4: Does the school inform the user that the identity provider will transfer its personal data to a specific Service Provider?

To investigate the targeted actions that schools implement to manage identity, a specific question was included about what steps have been taken to ensure the continuity of authentication and authorisation. Schools responded:

- Infrastructure fault tolerant 34,5%
- Disaster recovery plan 21.8%
- Multiple IdP instances 7,3%
- None 49.1%
- Don't Know 5.4%

The trend of responses does not change in relation to security actions, and there is also a lack of attention in identity management.

More than 50% of respondents, for example, declare that failure or non-maintenance operations that may cause interruptions or changes to the service are provided earlier and users are informed

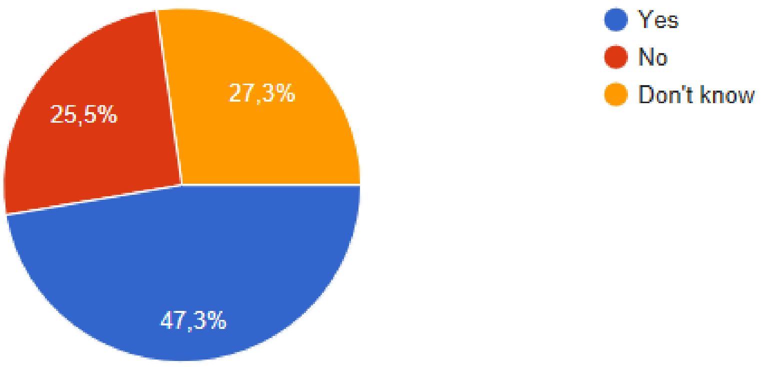

Figure 4.5: Maintenance operations that may cause interruptions or variations of the service: are they previously scheduled and the users warned?

However, 70.3% of the respondents state that the message that warns users of error or malfunctions is a generic "error related" thing that nothing specifies about the problem actually encountered:

The messages that the IdP (Identity Provider) returns to the user in case of error or malfunction are:

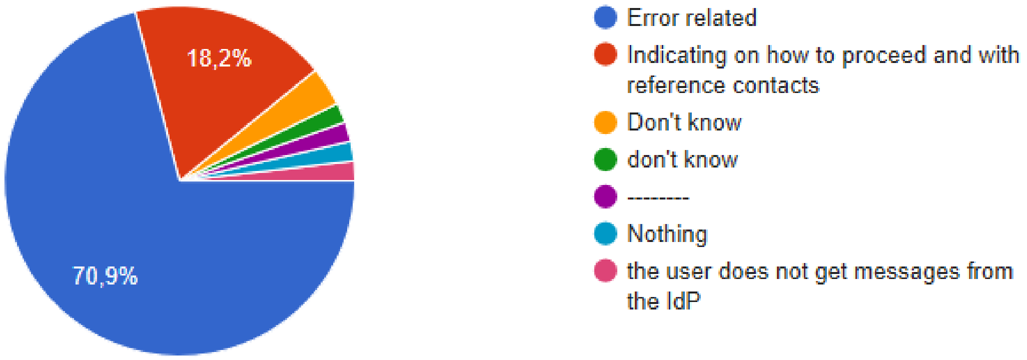

Figure 4.6: The messages that the IdP (Identity Provider) returns to the user in case of error or malfunction are:

Finally, just over 50% of respondents do not know if they claim credentials maintained by identity management systems are not safely transmitted and shredded:

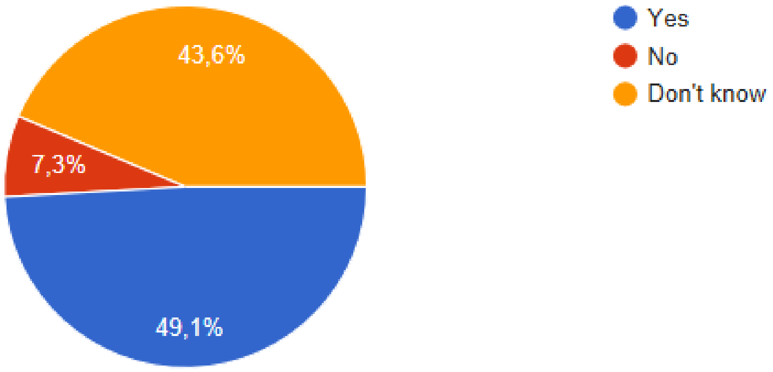

Figure 4.7: Are the credentials kept by Identity Management systems always safely transmitted and encrypted?

4.8 Authentication and Authorisation Infrastructure (AAI) for Up2U

4.8.1 The Model

The key objective of Up2U is to bridge the gap between schools and higher education primarily by adopting technology and infrastructure that is the underlying foundation of the global research and education community.

When it comes to authentication (AuthN) and authorization (AuthZ) solutions for the federated and integrated Up2U next generation learning platform and its services, Up2U is going to follow the state-of-the-art architecture and guidelines recommended by the flagship project AARC (and lately AARC2) [17-28].

AARC (Authentication and Authorization for Research and Collaboration) [AARC] is an EC funded project that brings together 20 different partners from among National Research and Education Networks (NRENs) organisations, e-Infrastructures service providers and libraries, including those who are also participating in Up2U.

AARC published its latest Blueprint Architecture (AARC-BPA-2017) in June 2017 (Figure 4.8). The purpose of the BPA [BPA] is to provide set of interoperable architectural building blocks for software architects and technical decision makers, who are designing and implementing access management solutions for international research and education collaborations, just like Up2U does it for the K12 education space.

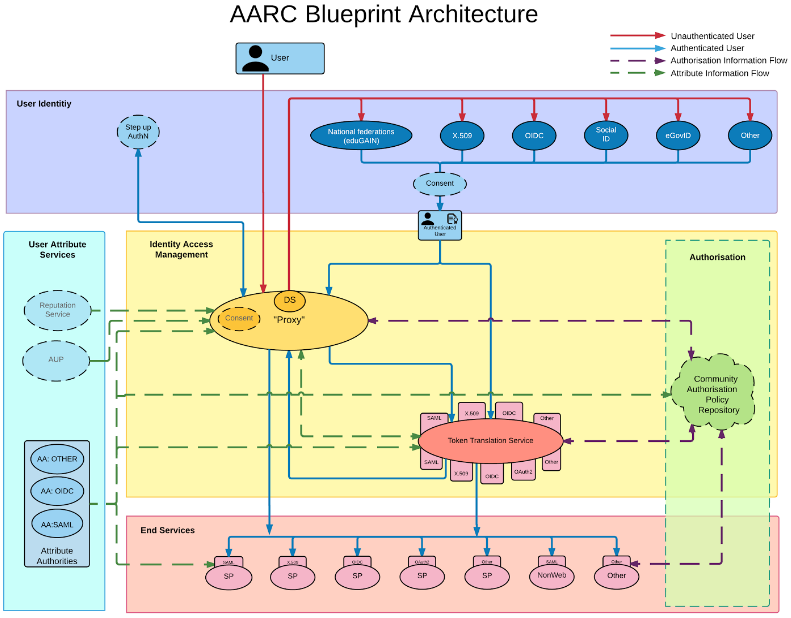

Figure 4.8: AARC Blueprint Architecture 2017

This version of the AARC Blueprint Architecture (AARC-BPA-2017), builds upon the previous one and provides a more detailed layered architecture, while retaining full backwards compatibility. AARC-BPA-2017 retains the same four layers, each of which includes one or more functional components, grouped by their complementary functional roles. The User Identities layer and the End Services layer are still there, while the Attribute Enrichment layer has been renamed to User Attributes layer and the Translation layer has been renamed to Identity Access Management (IAM) Layer and has a prominent role in the architecture. In AARC-BPA-2017, a new layer for the centralised Authorisation has been introduced.

Authentication for the initial pilot phase has been reported in Deliverable 4.1 (Application Toolbox Design and Prototype).

4.8.2 Next Steps

Shortly after launching the first pilot phase, we are going to experiment with another AAI solution (provided by GWDG) including the “Step up AuthN” feature of the Blueprint Architecture that will allow the “homeless” schools on our platform (in case if they are accepting and trusting our personal data protection policies).

4.8.3 Solutions for Authorisation

The authorisation layer of the Blueprint Architecture is not implemented by the current GÉANT Service Provider Proxy. In the initial pilot phase, after federated authentication, the AuthZ function will be provided by Moodle. This is of course not modular and scalable for the project. Just like AuthN, our vision is that the AuthZ functionality will also be externalized.

We are currently investigating various software products and initiatives to implement externalized AuthZ function for Up2U. The options are:

a) Grouper is an enterprise access management system designed for the highly distributed management environment and heterogeneous information technology environment common to universities and schools [23].

b) COmanage, a project funded by the NSF and Internet2, is a collaboration management platform that allows organizations to meet their science and research objectives using key collaboration tools in a secure and effective framework. By leveraging federated identity management services, the authentication and authorization of Collaborative Organization (CO) members are handled in a single, efficient process defined by the CO [24].

c) With SURFconext Authorisation Rules, which are available as standard in SURFconext, institutions can decide for themselves whether to make a service connected to SURFconext accessible to everyone or whether to restrict access to a specific group of users. This can easily be implemented via the SURFconext Dashboard [25].

d) eduTEAMS gives the capability to build, manage and control virtual teams. Built on top of eduGAIN, eduTEAMS aims to simplify the management of group and authorisation information. It enables the integration users from a wide range of environment, connecting them to specific services (such as Up2U), and also to other generic services such as storage and compute provided by any e-Infrastructure provider or even commercial entity [26].

4.8.4 Grouper/COmanage Pilots

In the initial pilot phase, we are going to experiment with the Moodle platform and its authorisation and group management features. Shortly after the launch, we are going to experiment with the integration of Moodle and Grouper – already tested by GARR [27]. The schematic architecture of the proposed option is depicted on Figure 4.9.

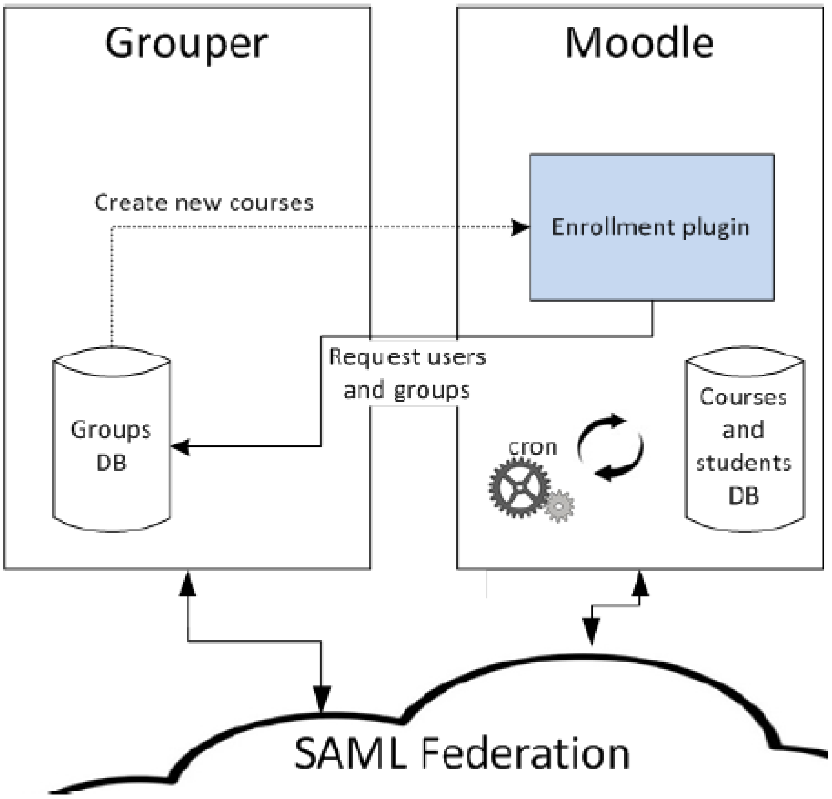

Figure 4.9: Moodle and Grouper integration

GÉANT is also running an instance of COmanage [28]. It is possible to create a virtual "Up2U Collaboration" in the GÉANT COmanage platform and hook it up with Moodle easily. This allows us to compare the COmanage solution with Grouper and decide which option will be chosen for the next pilot phase.

4.8.5 Roadmap

Table 4.1 summarises the evolution of the Authentication and Authorization Infrastructure solutions implemented, tested and evaluated by Up2U in the first pilot phase (September 2017 – June 2018) We are committed to follow and comply with the AARC Blueprint Architecture, its guidelines and recommendations throughout the entire Up2U project.

Pilot phase I.	Platform(s) supported	Authentication	Authorization
Beginning of the first pilot phase (September 2017)	Moodle w/o eduOER	GÉANT SP Proxy and eduGAIN	Moodle
End of the first pilot phase	Moodle w/o eduOER, ownCloud and LTI Tools	GÉANT SP Proxy and eduGAIN	COmanage (GÉANT)

(June 2018)	PuMuKIT and OpenEdX Jupyter/EoS stack	GWDG SP Proxy with relevant IdPs and local LDAP	Grouper (GARR) eduTEAMS, if available

Table 4.1: AAI solutions to be deployed and evaluated during the initial pilot phase

The actual AAI solution to be used in the second pilot phase of Up2U will be determined based on the feedback and assessment of the aforementioned alternatives in Phase I.

Note that in the second phase of the pilot we envisage several Up2U service platforms hosted by NRENs or other organisations in the pilot countries working in a federated and distributed manner. The separate service platforms may implement different but interoperable AAI solutions suitable for the needs of the national pilot schools.

4.9 IdP in the Cloud

Identity federations are a benefit for the National Research and Education Networks (NREN) communities and core e-Infrastructure services [29]. Common protocols and attributes offer to the users more services and a simpler management of the credentials, while allowing service providers (SP) to reach a larger group of potential users. However, smaller institutions may struggle when setting up the tools needed to join a federation. The lack of resources, expertise and manpower can discourage the setup of an identity provider (IdP). The “IdP in the cloud” service has been developed to cope with these issues. The service relies on Infrastructure-as-a Service paradigm and Development-Operation methodology (DevOps) to automate and simplify the creation and the maintenance of an IdP appliance, letting the local account managers free to focus on the users accreditation and policies.

Consortium GARR, the Italian NREN, created and supports IDEM: an identity federation among the national universities and research institutions. IDEM fosters the effort of its community to define and support a common framework that allows users to access on-line resources through the unique identity their organization provides them. The federation adopts SAML2 as assertion exchange protocol with Shibboleth and simpleSAMLphp as favourite implementations. Thanks to the standard compliancy, IDEM is in line with other NRENs activities, is member of eduGAIN and participates to REFEDS.

Identity federations are not trivial to deploy and configure. This holds in particular for small organizations that cannot, or do not want, allocate time, money, and resources to understand SAML and AAI details. Instead, they would like to focus on account management getting only the pros of the federated services. Joining a federation implies also formal steps, like signed agreements and acceptance of policies that could slow down further the process. The overall complexity hinders the benefits of taking part to a federation, discouraging also new service providers in a vicious circle that keeps the participation below the desired levels. It is therefore essential to grant an easy access to the federation services for these non-ICT focused users.

GARR has developed the “IdP in the cloud” service to implement the efficient creation and configuration of new IdP virtual appliances in high availability, with identity management tools and monitoring. The service minimizes the manpower requirements and increases scalability, with few operators being able to administer hundreds of IdPs. The user’s tasks are reduced by 80% and the organizations are led to join the IDEM federation with a workflow completion time reduction of 88%. The user duties focus on initial provisioning of information about the organization and on the daily identity management once the IdP is delivered.

“IdP in the cloud” leverages IaaS cloud and DevOps agile methodology to provision new IdPs in a few minutes with a PaaS strategy.

GARR harmonized the following tools in a distributed infrastructure:

- OpenStack, used to create the VMs that host the IdP and the related networking properties like firewall rules, and IP address management;
- GlusterFS file system, to ensure resilient geographical replication of both the VM instances and live migration. GlusterFS is used also to persist organization data;
- On top of them, Puppet configuration manager installs and configures the software dependencies to deploy a Shibboleth IdP, an LDAP registry and web interfaces for monitoring and identity management. If the organization wants to use an external pre-existing identity base, Puppet either imports it or connects it to the IdP through a secure VPN channel according the user preference. Auxiliary tools like phpLDAPadmin, uApprove and custom login pages are deployed;
- Monitoring and alarming rely on Nagios, Collectd and Splunk. Both the user and the service operators are constantly informed on the status and the resource consumption of the IdPs.

Another advantage of the “IdP in the cloud” approach is that the IdPs have an inherently harmonized set of attributes and metadata, fulfilling since the beginning IDEM and eduGAIN recommendations. In addition, the metadata are automatically enriched as prescribed by REFEDS Discovery guidelines.

5 Content Policy

5.1 Intellectual Property Rights

Intellectual property refers to the output or creations for which ownership is assigned. This can include discoveries, inventions, music, words, phrases, symbols, code and designs. Copyright, in turn, is then the way in which the rights associated with these can be protected. While these concepts are fairly simple in some ways, the law that protects them is quite complex. There are sometimes different levels of legislation (for example national, European, and worldwide agreements can all be applied and may contain contradictions), the ownership may not be obvious, and exceptions that work in some cases may not in others. When copyright is applied to printed material these complexities cause relatively few problems, not least because the object itself is very apparent. Now that material is available on the Internet and materials are digital, problems are exposed more and more. Fortunately, there has also been work such as that supported by Creative Commons on sensible simplifications and establishing working practices that can apply for education.

All Creative Commons licenses have many important features in common. Every license helps creators retain copyright while allowing others to copy, distribute, and make some uses of their work, at least non-commercially. Every Creative Commons license also ensures licensors get the credit for their work they deserve. Every Creative Commons license works around the world and lasts as long as applicable copyright lasts. These common features serve as the baseline, on top of which licensors can choose to grant additional permissions when deciding how they want their work to be used.

In this section we explain different types of creative commons licences.

Each licence has its own icon. This is how to visually identify the license of each multimedia object.

Name: Attribution
Abbreviation: CC BY

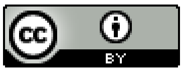

Figure 5.1: Attribution license representation (CC BY)

This license lets others distribute, remix, tweak, and build upon your work, even commercially, as long as they credit you for the original creation. This is the most accommodating of licenses offered. Recommended for maximum dissemination and use of licensed materials.

Name: Attribution-ShareAlike
Abbreviation: CC BY-SA

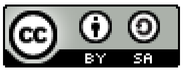

Figure 5.2: Attribution-ShareAlike license representation (CC BY-SA)

This license lets others remix, tweak, and build upon your work even for commercial purposes, as long as they credit you and license their new creations under the identical terms. This license is often compared to “copyleft” free and open source software licenses. All new works based on yours will carry the same license, so any derivatives will also allow commercial use. This is the license used by Wikipedia, and is recommended for materials that would benefit from incorporating content from Wikipedia and similarly licensed projects.

Name: Attribution-NoDerivs
Abbreviation: CC BY-ND

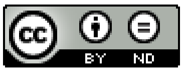

Figure 5.3: Attribution-NoDerivs license representation (CC BY-ND)

This license allows for redistribution, commercial and non-commercial, as long as it is passed along unchanged and in whole, with credit to you.

Name: Attribution-NonCommercial
Abbreviation: CC BY-NC

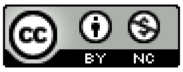

Figure 5.4: Attribution-NonCommercial license representation (CC BY-NC)

This license lets others remix, tweak, and build upon your work non-commercially, and although their new works must also acknowledge you and be non-commercial, they don’t have to license their derivative works on the same terms.

Name: Attribution-NonCommercial-ShareAlike
Abbreviation: CC BY-NC-SA

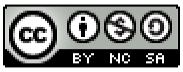

Figure 5.5: Attribution-NonCommercial-ShareAlike license representation (CC BY-NC-SA)

This license lets others remix, tweak, and build upon your work non-commercially, as long as they credit you and license their new creations under the identical terms.

Name: Attribution-NonCommercial-NoDerivs
Abbreviation: CC BY-NC-ND

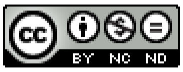

Figure 5.6: Attribution-NonCommercial-NoDerivs license representation (CC BY-NC-ND)

This license is the most restrictive of our six main licenses, only allowing others to download your works and share them with others as long as they credit you, but they can't change them in any way or use them commercially. You can check the license updates on this website [30].

5.2 Copyright or Copyleft

Copyright is defined as the set of norms and principles that regulate the moral and patrimonial rights that the law grants to authors, by the mere fact of the creation of a literary, artistic, scientific or didactic work, whether published or not unpublished.

We will define copyright, copyleft and creative commons and then discuss the differences.

Figure 5.7: Image of the copyright symbol

Copyright is the most popular license, and unfortunately, also the most commonly used. It allows full rights to the owner of the work (that may not be the very author), and he's the only one that may decide what to do with it, whether to charge for it or not, besides having to request permission for usage. Distribution is only restricted to the owner of the creation, that means the license only allows possession but not distribution. This is usually applied to books, music, movies and software, as an example.

Figure 5.8: Image of the Copyleft symbol

Copyleft is the mother license for Creative Commons, which is the opposite of Copyright. Works are not restricted by any constraint: they can be modified, shared with other users and content can be copied. Modification of original work may even be commercial.

The main difference between Copyleft and **Creative Commons** is that Creative Commons is more flexible than its father: level of protection can be set directly by the author of the work. There are different possibilities to establish what kind of constraints to attribute to a Creative Commons License, but all of them share one, that is acknowledging the author of the work. This is default obligation for the user. All other constraints are specified by the author. Following image sums up the features.

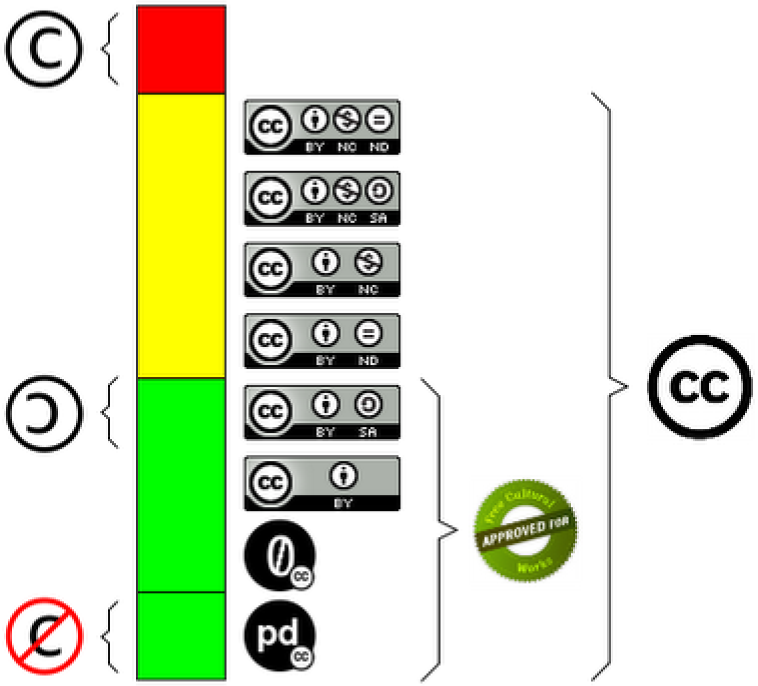

Figure 5.9: Sums up the features of Creative Commons

Last two indicate that the author does not keep any right on his work, basically the work is delivered as a World heritage.

"0" means that more than 70 years have passed since the author has passed away, while "pd" means that the work is already World heritage because the author indicated so.

5.3 IP Management in Horizon 2020

With Horizon 2020, the EU aims to strengthen the European scientific and technological base and fostering benefits for society as well as better exploitation of the economic and industrial potential of policies of innovation, research and technological development. In fact, it is essential that the public resources and efforts used in research are converted into socio-economic benefits to the EU. For this reason, Horizon 2020 establishes commitments from the participants in terms of dissemination and exploitation of the projects' results, including their protection through intellectual property.

As in FP7, under Horizon 2020, participants are obliged to exploit their own results, either commercially and in further research, or by establishing licensing deals, assignments or other partnerships to allow exploitation by other entities. However, a reservation is foreseen so that additional exploitation obligations may be laid down as part of the grant agreement. Moreover, it is clearly established that participants must use their best efforts in the exploitation of their own results. The general rule in terms of dissemination does not change as well: each participant needs to ensure that the results which it owns are disseminated as soon as possible and through appropriate means. However, dissemination is subject to the restrictions resulting from intellectual property protection, security rules or legitimate commercial interests.

We think the following labels are a good option to use:

- PU = Public
- PP = Restricted to other programme participants (including the Commission Services)
- RE = Restricted to a group specified by the consortium (including the Commission Services)
- CO = Confidential, only for members of the consortium (including the Commission Services)

The aim of labelling deliverables as "PU" or "Public" in this context is therefore to make clear between the participants and the European Commission that there are no restrictions on the people to whom the deliverable can be disseminated. However, this does not mean that in a public deliverable there are no intellectual property rights, particularly copyright. In fact, these are two different matters and the fact that the consortium has labelled a deliverable as public does not mean that the owner of the deliverable waives its copyright rights. The same principle applies to reports and other works made available on the internet.

In the European Union, copyright has the special characteristic of being an automatic right, namely that there is no need to seek registration. Copyright arises with the creation of the work, provided that the work is original. Consequently, once a deliverable is written, it is automatically protected by copyright as long as it is considered original. This special characteristic of copyright has impact at several levels.

5.4 Open Educational Resources

Higher education institutions worldwide have been using digital technologies to create, archive and disseminate multimedia learning materials for a number of years. Only lately, i.e. within the last ten years, have Open Educational Resources (OER) gained momentum in association with the current wave of enhancing the public domain, aimed at granting universal and open access to research and learning digital material.

The Paris OER Declaration, adopted during a UNESCO meeting in 2012, constituted a major step in the progressive development of policies supporting and fostering the use of OER. The Declaration marked “a historic moment in the growing movement for Open Educational Resources and calls on governments worldwide to openly license publicly funded educational materials for public use” (UNESCO, 2012) [31]. UNESCO member States were prompted to foster awareness and use of OER, promote the understanding and use of open licensing frameworks and facilitate finding, retrieving and sharing of OER; in short, the Paris Declaration invited member States to encourage the open licensing of educational materials produced with public funds.

The term OER “was meant to emphasize knowledge construction as an ongoing process that required editable, digital materials more in keeping with the dynamics of online learning and teaching” (Blyth,

2012) [32]; it now refers to any kind of educational resources that are openly available for use by educators and students, without an accompanying need to pay royalties or licence fees. In a nutshell, an OER is "simply an educational resource that incorporates a licence that facilitates reuse, and potentially adaptation, without first requesting permission from the copyright holder" (Butcher, N., Kanwar, A., & Uvalic-Trumbic, 2011) [33]. Therefore, "every person in the world enjoys free (no cost) access to the OER and free (no cost) permission to engage in the 4R activities when using the OER: revise—adapt and improve the OER so it better meets your needs, remix—combine or "mash up" the OER with other OER to produce new materials, reuse—use the original or your new version of the OER in a wide range of contexts, and redistribute—make copies and share the original OER or your new version with others" (Wiley and Green 2012, p. 81) [34].

The use of OER in educational courses, through resource-based learning means, is proportional to the ease of use of digitized resources, multimedia objects in particular, via the Internet. Resource-based learning should not be thought of as an alternative to replace traditional education; rather, by enabling the friendly use of digital technology to facilitate the learning process through the use of different media, resource-based learning constitutes a complementary way of teacher-student interaction which is bound to become a key component of any formal education program.

5.5 Curation of OER

An important part of the success of any OER endeavour is to safeguard the sustainability, beyond the lifetime of the project, of all the learning resources that are going to be deployed. To that end, it is necessary to incorporate basic curation tasks, targeting the appropriate content selection and annotation, to enable the creation of the learning environment.

However, we understand OER curation in a much broader sense. In addition to carry out the recommendations from international organizations on ethical issues, concerning open licensing, copyright policies, access control, and privacy rights, curation policies should facilitate the following experiences of the various stakeholders of the teaching/learning community:

- ***For students/researchers:*** better access to an extensive pool of multimedia multilingual OER that can enrich learning, especially video lectures, practical experiences and tutorials.
- ***For content providers:*** better visibility of their content, in some cases presenting material that has never been linked or findable before; metadata harvestable by other services; metadata quality control; metadata analytics and visualization; tools for improvement of metadata feedback and updating.
- ***For professors:*** better access to teaching material, support for online courses and blended learning, combining face-to-face learning with additional digital resources.
- ***For institutions:*** learning materials shared with other institutions, promotion of the use and reuse of learning resources, increased exposure of the institution to the public and to potential students within an environment based on a trusted repository.
- **For other OER aggregators: availability of open source software and more OER metadata.**

In this context, we see curation as an integral part of the normal workflow of data creation and managing of open educational resources, much in the same way as what Miles (2007) dubbed sheer curation or curation at source, a "lightweight and virtually transparent" curation process based upon the hypothesis that "good data and digital asset management at local levels is also good practice in preparing for publication and/or preservation of data and other digital assets". The success of this approach to digital curation, where "curation activities are quietly integrated into the normal workflow of those creating and managing data and other digital assets", relies on "curators having close contact or 'immersion' in data creators' working practices" (UX thesis, 2012) [35].

The first step in the curation process is therefore to ensure the quality of the metadata since it will help primary users to effectively make use of the data held in the repository, and secondary users to understand and reuse such data. The most accurate providers of metadata are by and large the content creators themselves; hence, the OER service architecture should enable content creators to seamlessly add metadata to their learning objects. Besides, using the appropriate technology at the recording point is of utmost importance.

Additionally, we believe that collecting information from secondary users (para-data), including the context in which the material has been reused, along with feedback from both teachers and students, can and should be effectively used to enhance the metadata of the learning objects, completing a virtuous circle that would benefit the value and trustworthiness of the repository. There are then a number of activities around the learning objects from an OER service that need to be properly managed through a feasible operational workflow. Moreover, emerging Multimedia OER's, like Up2U, need to create, manage and integrate a great deal of multimedia content, resulting in a substantial increase of metadata generation tasks. The use of Opencast Matterhorn, a flexible and customizable video capture and distribution system built by a growing community of developers (Opencast, 2016) [36], ensures within Up2U the extraction of metadata in an automated way through the video content itself and/or the inclusion of appropriate QR coding for the teacher and the course. However, in order to streamline the workflow of the multimedia content creation, we need to connect the multimedia recording with the repository and the particular learning management system (LMS) to which the multimedia object is going to be added.

Hence, our ideal architecture should facilitate the task of the content creators by providing an appropriate connection of all the elements of the OER service with the central repository.

5.6 Application-Linked Repository to Facilitate Curation at Source Through Various User Experiences

Curation in an OER service is made easier if all the learning objects are stored in a centralized repository. The idea of an integrated content repository was first introduced in 2006, within the context of information management, through MIKE2, an open source methodology that provides a framework for information development and management. In MIKE2 the repository is "a federated hub of shared assets from the Internet and content held internally by an organization" (Rindler et al 2013). The idea of an integrated repository has also been used in the context of application delivering to managed devices via HTTP protocol (Zenworks 2017) [37].

Some of the benefits from a strong integration of content in a central repository have been extensively reported in the literature. Centrally controlled and integrated systems, provided with powerful, flexible, consistent searching and browsing, may come at a high cost –their content should be proactively managed to enable reliable validation data processes (Awad, 2007) [38]– but will ensure high usability (Morville & Rosenfeld, 2007) [39]; Shivakumar (2016) reports that a centralized repository, integrating content from different sources, is a safe way to enable the implementation of a robust content reusability strategy. An institutional implementation of a strongly centralized and integrated information management system reported by Ashfari & Jones (2007) [40] demonstrated the "advantages of producing integrated systems, especially with regard to lowering adoption barriers through easing academics' deposit workflows".

Institutions concerned with generating, preserving, and disseminating open educational resources encourage their faculty to share the learning materials they create and use in the classroom by way of specific policies and guidelines. Since institutions are very well aware of the benefits of a centralized repository, faculty in charge of generating open educational resources for their LMS institutional platform are usually asked to carry out an additional task: cataloguing the learning objects and uploading them into a centralized institutional repository, thus facilitating their proper identification, access and reuse by third parties. If the learning objects are to be placed in a central repository, faculty will have to deal with the standard curation procedures associated with the creation of educational resources as well as with the institutional recommendations for managing ethical issues pointed out in Section 2.

It is therefore clear that content creators would greatly benefit from receiving institutional support to understand the underlying copyright guidelines behind open-access archiving, as well as to realize the potential benefits derived from the use of well-crafted, user-friendly interfaces to facilitate the integration of the content into the central repository. In spite of receiving that kind of support it is apparent that the extra step of caring about the objects to be placed into the institutional repository requires a very demanding additional effort from the teachers without providing any obvious added value to their daily duties. This is, we believe, the reason behind the lack of success of many such institutional repositories, including integrated content repositories, since only a few faculty will, by and large, take the necessary extra step to properly catalogue and upload the material to the central repository, no matter the willingness to share.

Being the repository in a position to integrate all the learning objects used in the system is therefore a necessary but not a sufficient condition for the solution to the curation at source problem we have outlined above. Within Up2U we understand that a new architecture for the OER service, in which the central repository can effectively become the curation hub, is the best path to success.

The application-linked repository

To make the central repository play the role of a central hub for curation, we propose to link it with the applications by means of suitable plugins to streamline curation at source: those plugins should enable content creators (usually the faculty from an institution) to help in upgrading the repository without any extra effort, as figure 10 shows.

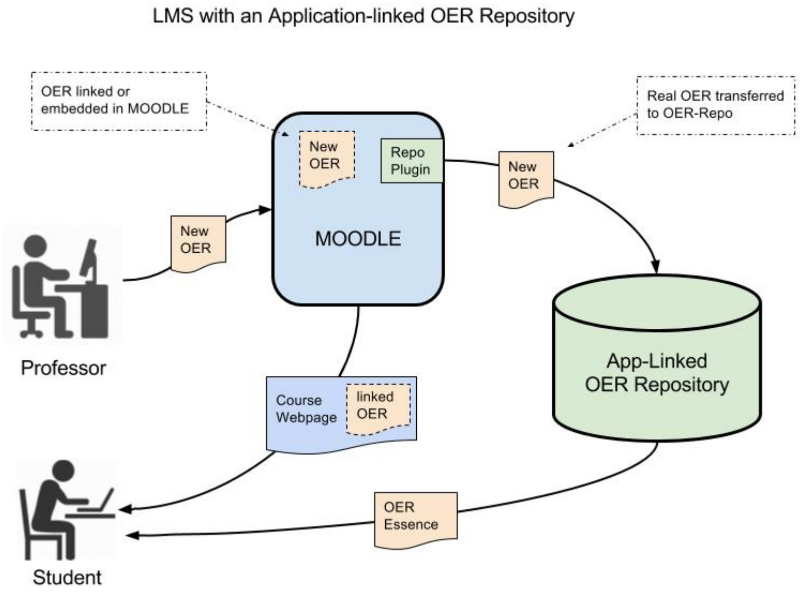
LMS with an Application-linked OER Repository
OER linked or embedded in MOODLE
Real OER transferred to OER-Repo
New OER
Repo Plugin
MOODLE
New OER
New OER
Professor
App-Linked OER Repository
Course Webpage
linked OER
OER Essence
Student

Figure 5.10: Application-Linked Repository workflow

Within an architecture in which an application-linked repository takes a central place, content creators will not need any extra effort to add objects to the repository; their daily experience within their institutional online teaching platform will remain the same; as a matter of fact, they will think they are just uploading the learning materials to their courses through the institutional LMS (Moodle, Sakai, OpenEdX, etc.) when in fact the materials are first being stored and catalogued in a repository, external but linked to the LMS, and then seamlessly added to the teacher's online platform.

This is the "Application-linked Repository" architecture that we propose for our project and for any OER service. The success of this architecture is based on the curation at source approach discussed in point 5.5. By connecting the repository to the LMS, we make sure that any modification in the metadata of a learning object the teacher makes in the LMS (as simple as a title spelling correction, for instance) will be automatically transferred to the repository. Since all the elements of the OER service will be connected with the repository in a seamless way, simple and effective guidelines can be designed to facilitate curation at source, including provisions for ethical issues that would be easily conveyed to content creators.

The use of data analytics may also help institutions to manage their OER effectively. Analytics map how visitors move through content, leading to the identification of the areas and resources which attract the most interest from users (Scime, 2009) [40]. By connecting all data analytics with the application-linked repository, the additional data supplied by courses which make use of the open educational resources will enhance, without any extra work, the quality and reusability of the repository; such data (para-data) may be used to update and enhance the metadata of the open educational resources, thus placing the repository in a better position for being identified and accessed. We refer here for instance to course titles, course level of complexity, or number of courses in which the OER has been included. Moreover, the valuable information data analytics convey would seamlessly be passed on to the content creators through the learning management systems.

The architecture has already been tested, in a preliminary setting, at the University of Vigo web Tv Portal, in which an open source video platform to manage large media repositories has been in operation for more than five years. The platform (PuMuKIT, 2015) [42] includes an integration module with Opencast-MH, and has also been adopted by GÉANT as the front end of its OER repository (eduOER, 2016) [43].

5.7 How Ethical Committees Work in Universities

We are fully aware of the need to adopt clear licensing as well as sound copyright policies within the Up2U multi-institutional consortium. We start by acknowledging the relevant recommendations from OECD, UNESCO and the European Union, starting from the applicable principles and standards established by the OECD to facilitate access to research data generated with public funding. Furthermore, we take notice of the General Data Protection and Regulation (GDPR) approved by the European Union Parliament on 14 April 2016. The GDPR, designed to harmonize data privacy laws across Europe, will have direct application in all member states in two-year time. Because we believe that trustworthiness is a quality of utmost importance at present, we acknowledge as well the guidelines produced by the European Framework for Audit and Certification of Digital Repositories.

Ethical issues affect how data is stored and how long it is kept. Managing ethical concerns include provisions for acknowledging intellectual property rights, anonymization for data analytics, and formal consent agreements, particularly when some of the users are very young. We summarize below some principles and guidelines of application to the management of ethical issues in OER services:

- **OECD, 2007, Principles and Guidelines for Access to Research Data from Public Funding, (OECD, 2007)** [44]

Encourage open access in the broadest possible form, ensuring privacy and confidentiality, respecting the legal rights and legitimate interests of all stakeholders. Adopt data access arrangements which describe good practices for methods, techniques and instruments employed in the collection, dissemination and accessible archiving of data. Subject the performance of data access arrangements to periodic evaluation by user groups, responsible institutions and funding agencies.

- **New General Data Protection and Regulation (GDPR, 2016)** [45]

GDPR pertains solely to the protection of information that can be used to directly or indirectly identify the person. Identification should be allowed for only as long as is necessary. Consent must be clear and distinguishable from other matters. Any person has the right to obtain confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. No notifications/registrations of processing activities will be needed, just internal record keeping requirements.

- **European Framework for Audit and Certification of Digital Repositories. (TDR, 2017)** [46]

A transnational open educational resources service should actively pursue the maximum level of recognized trust. To that extent, we think that a great deal of attention should be paid to the guidelines produced by the European Framework for Audit and Certification of Digital Repositories, as defined in the memorandum of understanding signed in July 2010 between several working groups interested in setting up appropriate standards to recognize trusted digital repositories. The framework establishes three certification levels:

- Basic: self-assessment following the Data Seal of Approval (DSA, 2009) [47] requirements.
- Extended: externally reviewed self-audit against ISO 16363 (ISO, 2012) [48] or DIN 31644 (DIN, 2012) [49] requirements.
- Formal: validation of the self-certification with a third-party audit based on ISO 16363 or DIN 31644

- **Edinburgh: Digital Curation Centre (DCC, 2013) [50]**

Digital curation involves maintaining, preserving and adding value to digital data throughout its lifecycle. Since OERs resources are going to be reused for educational purposes, part of the curation is to prepare the data for sharing and preservation, including provisions for changing file formats if needed. We summarize below some steps in the digital curation lifecycle, taken from the DCC guidelines, which we consider relevant for our project.

1. Assign administrative, descriptive, structural and technical archival metadata to digital objects.
2. Transfer digital objects to a trusted digital repository.
3. Undertake actions to ensure the long-term access and preservation of digital objects.
4. Create new digital objects from the original, for example, by migration into a different form.

5.8 Intellectual Property Rights: Findings From Survey Analysis

80% of teachers use network downloaded resources for their lessons (18.2% don’t know), as shown in Figure 5.11. 39 out of 47 (83%) download resources under Public domain license; 34 out of 47 (72.3%) under Creative Commons license; 22 out of 47 (46.8%) download resources with “fair use of copyrighted content”; 9 out of 47 (19.1%) download resources fully covered by copyright.

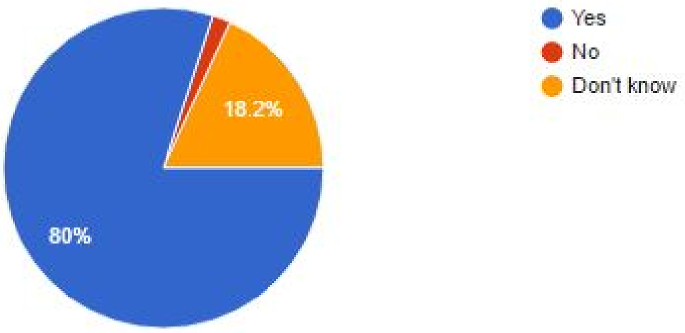

Figure 5.11: Do your school teachers and students use resources (texts, videos, images ...) downloaded from the network for their lessons?

52.7% of respondents said their school did not have management policies for the resources downloaded from the network with educational and didactic aims (Figure 5.12); 38.1% don't know and only 9.1% answers "yes".

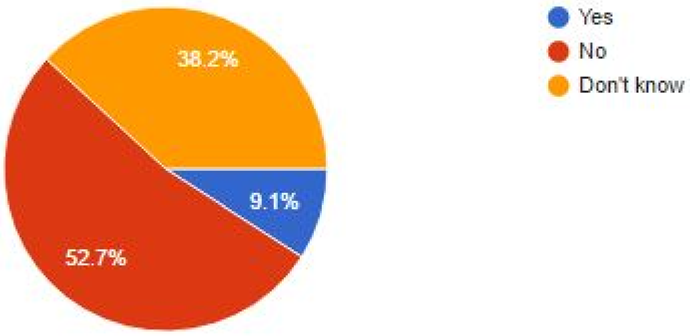

Figure 5.12: Do you have a management policy for the resources downloaded from the network for educational and didactic aims?

When asked if their school uses Open Educational Resources, 49.1% answered they don't know; 30.9% answered "no" and only 20% answered affirmatively (Figure 5.13). Note that in the following open-ended question, "If you answered yes, indicate three repositories/aggregators from which you download OERs", some answers (2 out of 8) indicate YouTube as an OER.

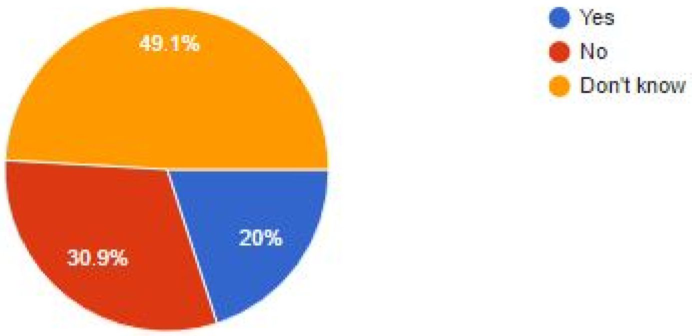

Figure 5.13: Does your school use OER (Open Educational Resources)?

85.5% of respondents said their school teachers and students produce educational resources with materials downloaded from the network (Figure 5.14) and they use them mostly for their own school without sharing them online (Figure 5.15).

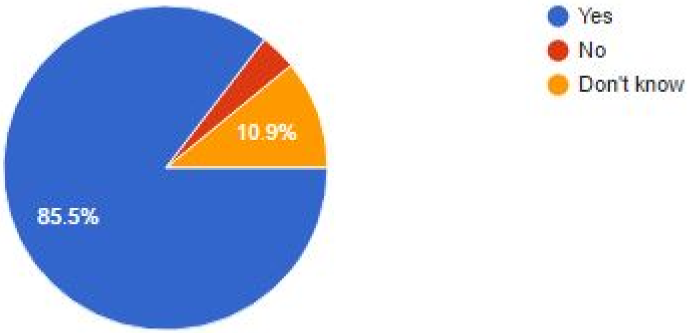

Figure 5.14: Do your school teachers and students produce educational resources with materials downloaded from the network?

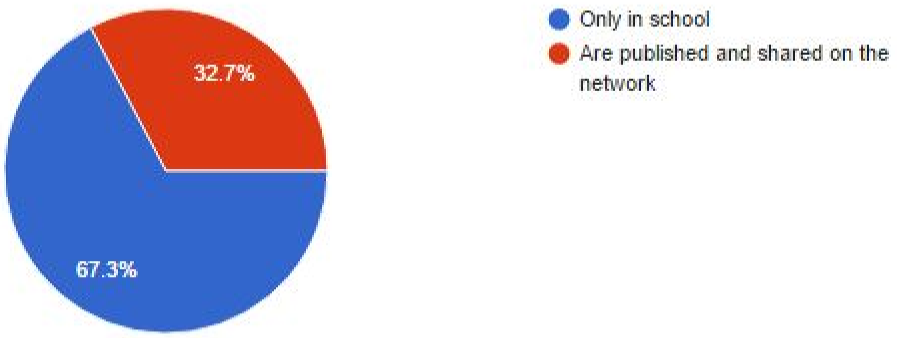

Figure 5.15: Are your produced educational resources only used in your school or do you publish and share them online?

25 out of 39 respondents (64.1%) share their produced OER with Creative Commons licensing; 17 out of 39 (43.6) with Public domain licensing and 9 out of 39 (23.1%) with copyright. When asked "How do you share them", 30 out of 55 answer (54.4%) via mail; 29 out 55 (52.7%) on their school's website; 28 out of 55 (50.9%) in cloud and 24 (43.6%) via social networks.

6 Conclusions

This deliverable aims to depict reality of schools in the countries involved [51] in the UP2U project in relation to the issues of ICT security, identity management, intellectual property and privacy.

These themes are interlinked with the ultimate aim of the whole project, which is to create a technological and pedagogical bridge between high schools and universities. The use of ICT in schools, especially because of students' young age, cannot ignore the full awareness of their use by teaching staff. The latter must have all the tools to choose the functional technologies for achieving didactic objectives, without neglecting the rules underlying their operation.

The analysis led to a tendency towards "ingenuity" by school institutions in the use of networked teaching technologies and materials.

By diving into certain dynamics and some educational processes, this document stated the need to keep up with the times and the will to respond to the needs of students, increase exponentially the risk of misuse of teaching technology.

For this reason, in the next months, after a study of the scope and requirements from NRENs' experiences, and the analysis and tests defined in the GÈANT project activities, we will prepare an executable roadmap for security, privacy and identity and access management in the UP2U ecosystem.

Appendix A General Data Protection Regulation

A.1 General Principles

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA - *Article 5 GDPR:*

1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); 4.5.2016 L 119/35 Official Journal of the European Union EN (1)Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). 2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Lawfulness of processing - *Article 6* (see also: "second part – **B. – Consent").**

1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) *processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.*

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: (a) Union law; or (b) Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific 4.5.2016 L 119/36 Official Journal of the European Union EN processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued. 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

***Conditions for consent:** Article 7* (see also: "second part – **B. Consent"**.

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2.If the data subject's consent is given *in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3.The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4.When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

A.2 GDPR

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case.

Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

<u>(art. 15). *The data Subject, has the right to access to the personal data and the following information:*</u>

(a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given 4.5.2016 L 119/12 Official Journal of the European Union EN his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual *orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.*

WOUNDS OF RIGHTS TO BE PROTECTED:

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

ARTICLE 32 SECURITY OF PROCESSING:

1. *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
    a. *the pseudonymisation and encryption of personal data;*
    b. *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
    c. *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
    d. *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*
2. *In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
3. *Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.*
4. *The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.*

Art. 25 GDPR - Data protection by design and by default.

1. *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*
2. *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*
3. *An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.*

(76) *The likelihood and severity of the risk to the rights and freedoms of the person concerned should be determined by reference to the nature, scope, context and purposes of data processing. Risk should be evaluated on the basis of an objective assessment by which it is established whether data processing operations involve a risk or a high risk.*

Appendix B Data Management Plan

B.1 Data Summary

The key objective of the Up2U project is to bridge the gap between secondary schools and higher education and research by better integrating formal and informal learning scenarios and adapting both the technology and the methodology that students will most likely be facing in universities. The project is focusing on the context of secondary schools. The learning context from the perspective of the students is the intersection of formal and informal spaces, a dynamic hybrid learning environment where synchronous activities meet in both virtual and real dimensions. Up2U is developing an innovative ecosystem that facilitates open, more effective and efficient co-design, co-creation, and use of digital content, tools and services adapted for personalised learning and teaching of high school students preparing for university. The project addresses project-based learning and peer-to-peer learning scenarios.

Up2U provides as part of the aforementioned ecosystem a learning management system (LMS) that integrates tools and applications provided by the project. Activities executed by students or teachers through any of these tools or application are logged and stored in the Learning Record Store (LRS). The data objects collected in the LRS therefore capture all the learning activities in the Up2U ecosystem. These objects are defined within the project as *Category-1* data. The purpose of the collection is to provide a large, comprehensive and integrated set of data featuring activities in formal and informal learning spaces. This data set is of high interest to learning analytics researchers. The types and formats of the respective data objects are not yet defined as the ecosystem is still under development. Protocol-wise, the eXperience API (http://tincanapi.com/overview/) will be used to collect the data with the respective data types still to be defined. The expected size of the data set is also unknown as of today, but it is expected that the overall size of the raw activity data will be in the range of Terabytes. Any further details and changes related to Category-1 data will be reported in future version of this document.

Up2U conducts surveys to gather information about the ICT situation of schools as well as their needs, and also to get opinions of responsible people at schools regarding open educational resources, security and privacy, IPR, and the upcoming GDPR. This data is defined as *Category-2*. The purpose of collecting this data is to design, implement, and deploy an Up2U infrastructure that fulfils the needs of the schools. Furthermore, this data offers a unique opportunity to decision makers, governments, and the schools itself to learn about and understand the situation at European schools from the perspective of Up2U. The data is collected through Google Forms (https://www.google.com/forms/about/) and stored as Microsoft Excel file. The overall size of the survey data is in the range of Megabytes. Any further details and changes related to Category-2 data will be reported in future version of this document. Furthermore, new Categories of data, which are collected or generated within the project, will be added to the data management plan.

As of today, Up2U has not re-used any particular data objects from other third parties (but software, tools, applications, and infrastructures), but it will in future if appropriate. Any re-use will be reported in future versions of this document at:

https://wiki.geant.org/display/UP2U/Data+Management+Plan

B.2 FAIR data

Regarding means to find, access, make interoperable, and re-use the data collected by Up2U, the two categories are handled differently. Category-1 data objects are of interest for researchers and therefore have to be made findable, accessible and interoperable, and their re-use will be fostered. Category-2 data objects are used internally in the Up2U project and mainly the knowledge derived from them will be published. Any sharing of the basic Category-2 data objects is not yet planned.

Any future updates of the FAIR handling of Category-1 and Category-2 data objects will be reported in this document.

B.2.1 Making data findable, including provisions for metadata

B.2.1.1 *Category-1 data objects*

As the Category-1 data objects are not fully specified regarding their type and format, it is too early to provide information regarding “making data findable”. Up2U will, however, make sure that suitable identifier and metadata standards or best practices will be applied.

B.2.1.2 *Category-2 data objects*

The data objects of this category are not shared.

B.2.2 Making data openly accessible

B.2.2.1 *Category-1 data objects*

Category-1 data will be made accessible. As the Category-1 data objects are not fully specified regarding their type and format, it is too early to provide information regarding the accessibility. Up2U will take care that a suitable repository is chosen depending on the requirements of the research community. It is envisaged that no particular software will be necessary to access the data. Up2U will make sure that the published data will not contain any personal data. It is therefore currently not planned to implement a data access committee or restrict the data access as open access is preferred.

B.2.2.2 *Category-2 data objects*

The data objects of this category are not shared. They contain personal data about the people answering the surveys as well as their opinions. Furthermore, these data objects are generated to shape the Up2U ecosystem and are not research data to be shared per se. As stated above, anonymous statics derived from these objects might be of value to certain stakeholder, but they are results of an analysis proves and not the data objects themselves.

B.2.3 Making data interoperable

B.2.3.1 *Category-1 data objects*

As the Category-1 data objects are not fully specified regarding their type and format, it is too early to provide information regarding their interoperability. Up2U will, however, make sure that suitable standards are chosen wherever possible to ease interoperability.

B.2.3.2 *Category-2 data objects*

The data objects of this category are not shared.

B.2.4 Increase data re-use (through clarifying licences)

B.2.4.1 *Category-1 data objects*

As the Category-1 data objects are not fully specified regarding their type and format, it is too early to provide information regarding their re-use. Up2U will most likely license the data under a Creative Commons license and will not make any restrictions regarding the duration of their re-use. Further details have to be specified during the coming project months.

B.2.4.2 *Category-2 data objects*

The data objects of this category are not shared.

B.3 Allocation of resources

The costs for making data FAIR in Up2U depend mainly on the yet to be specified details of the data objects. This cost will be, for the lifetime of the project, covered by the Up2U consortium. The data management will be governed by WP 6. Regarding long-term preservation, the resources will be determined during the project life-time based on the cost.

B.4 Data security

Partner GWDG will make sure that data security and data protection is taking care of with respect to the data objects collected in the project. GWDG is a data centre and has the respective expertise handling inter alia data from medical and sociological research. With respect to the decision of which repository to choose, certification and data security will be taken into consideration.

B.5 Ethical aspects

The ethical issues identified with respect to Category-1 and Category-2 data have been set out in the confidential Ethic Deliverables: D9.1, D9.2 and D9.3.

Up2U will inform its users regarding the data collection details through the Learning Management System.

B.6 Other issues

No further issues have been identified so far.

References

[1] [Up2U] https://up2university.eu/
the objective of Up2U is to bridge the gap between secondary schools and higher education & research by better integrating formal and informal learning scenarios and adapting both the technology and the methodology that students will most likely be facing in universities.

[2] Robinson, Ken, Lou Aronica, Creative schools: the grassroots revolution that's transforming education, 2015

[3] http://bit.ly/2ud5zyE

[4] Being young in Europe today - digital world – EUROSTAT website

[5] Mascheroni G., Cuman A., Net Children Go Mobile Final Report, 2014

[6] Students, Computers and Learning: Making the Connection, 2015, OECD

[7] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[8] https://en.wikipedia.org/wiki/Logical_security

[9] Mascheroni G., & Ólafsson K., Mobile internet access and use among European children. Initial findings of the Net Children Go Mobile project, 2013

[10] Attewell J., BYOD: a guide for school leaders, 2015, European Schoolnet

[11] http://www.sch.gr/

[12] Security aspects of virtualization, ENISA, 2017

[13] AA. VV., Challenges for trustworthy (multi-)Cloudbased services in the Digital Single Market, 2016

[14] Education on the Cloud 2014: State of the Art, 2014, School on the Cloud Network

[15] Norberto Nuno Gomes de Andrade, Shara Monteleone, Aaron Martin, Electronic Identity in Europe: Legal Challenges and Future Perspectives (e-ID 2020), European Commission Joint Research Centre Institute for Prospective Technological Studies, 2013

[16] Federated identity management from University to digital school, and one login to resources and services, Maria Laura Mantovani, Consortium GARR, Italy

[17] Authentication and Authorization for Research and Collaboration

[18] AARC Blueprint Architecture 2017 AARC-BPA-2017

[19] Moodle - Open Source Community

[20] Moodle Shibboleth plug-in

[21] GÉANT Service Provider Proxy

[22] eduGAIN service

[23] Grouper community

[24] COmanage

[25] SURFnet's solution

[26] eduTEAMS pilot

[27] HowTo Integrate Moodle with Grouper

[28] COmanage at GÉANT

[29] Farina F., Biancini A., Mantovani M. L., Malavolti M., Mandato P., Valli C., Prete L., Tomassini S., IdP in the Cloud - Federated identity management as a service at GARR, 2014

[30] https://creativecommons.org/licenses/?lang=en

[31] UNESCO (2012), Paris Declaration on Open Educational Resources

[32] Blyth, C. S. (2012), Open Educational Resources (OER), The Encyclopedia of Applied Linguistics, John Wiley & Sons, Inc

[33] Butcher, N., Kanwar, A., & Uvalic-Trumbic, S. (2011). Basic guide to open educational resources (OER), Commonwealth of Learning (Canada), Paris, UNESCO; Vancouver, COL.

[34] Blyth, C. S. (2012), Open Educational Resources (OER), The Encyclopedia of Applied Linguistics, John Wiley & Sons, Inc.

[35] UX thesis (2012), Sheer Curation, Retrieved on March 29 from http://www.uxthesis.com/2012/sheer-curation/

[36] Opencast (2016)

[37] Zenworks (2017), ZENworks Configuration Management: Content Management. Retrieved on March 28, 2017 from https://www.novell.com/documentation/zenworks2017/zen_cm_deployment_bp/data/b18zqk2d.html

[38] Awad, E.M. (2007), Knowledge Management, Pearson Education India

[39] Morville, P., Rosenfeld, L. (2007), Information Architecture for the World Wide Web: Designing Large-Scale Web Sites, O'Reilly Media, Inc.

[40] Afshari, F. and Jones, R. (2007), Developing an integrated institutional repository at Imperial College London, Program 2007 41:4, 338-352.

[41] Scime, E. (2009), The Content Strategist as Digital Curator, A List Apart. Retrieved on March 24, 2017 from https://alistapart.com/article/content-strategist-as-digital-curator

[42] PuMuKIT (2015), University of Vigo

[43] eduOER (2016), The Open Educational Resource Hub & Portal Service of GÉANT, Retrieved on April 18, 2017 from https://oer.geant.org/about-eduoer/

[44] OECD (2007). OECD principles and guidelines for access to research data from public funding. Retrieved on March 29, 2017 from http://www.oecd.org/science/sci-tech/oecdprinciplesandguidelinesforaccesstoresearchdatafrompublicfunding.htm

[45] GDPR (2016), Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. European Parliament & Council, L119, 4/5/2016, p. 1–88. Retrieved on March 28, 2017 from http://www.eugdpr.org/

[46] TDR (2010), European Framework for Audit and Certification of Digital Repositories, retrieved on March 24 from http://www.trusteddigitalrepository.eu

[47] DSA (2009), Data Seal of Approval requirements. Retrieved on March 28, 2017 from https://www.datasealofapproval.org/en/information/requirements/

[48] ISO (2012), International Organization for Standardization: ISO 16363:2012 Space Data and information trusted systems –Audit and certification of trustworthy digital repositories. Retrieved on March 27, 2017 from https://www.iso.org/standard/56510.html

[49] DIN (2012) DIN Standards Committee Information and Documentation; DIN 31644 Criteria for trustworthy digital archives. Retrieved on March 29, 2017 from http://www.din.de/en/getting-involved/standards-committees/nid/standards/wdc-beuth:din21:147058907

[50] DCC. (2013). Checklist for a Data Management Plan. v.4.0. Edinburgh: Digital Curation Centre. Retrieved on March 28, 2017 from http://www.dcc.ac.uk/resources/data-management-plans

[51] Netherlands, United Kingdom, Italy, Greece, Spain, Portugal, Israel, Lithuania, Hungary, Poland, Germany, Switzerland

Glossary

AAI	Authentication and Authorization Infrastructure
AARC	Authentication and Authorization for Research and Collaboration
AuthN	Authentication
AuthZ	Authorisation
BYOD	Bring Your Own Device
CO	Collaborative Organisation
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
eID	electronic IDentity
GDPR	General Data Protection Regulation
GÉANT SP	GÉANT Service Provider
GSN	Greek School Network
IAM	Identity Access Management
ICT	Information and Communication Technologies
IdP	Identity Provider
IoT	Internet of Things
IPR	Intellectual Property Rights
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
LMS	Learning Management System
MVP	Minimum Viable Product
NAS	Network Attached Storage
NAT	Network Address Translation
NRENs	National Research and Education Networks
OER	Open Educational Resources
PaaS	Platform as a Service
SaaS	Software as a Service
SAML	Simple Assertion Markup Language
SP	Service Provider
SSO	Single Sign On