United Nations
Educational, Scientific and
Cultural Organization

UNESCO Institute
for Information Technologies
in Education

Personal Data Security Technical Guide for Online Education Platforms

Published in 2020

by the UNESCO Institute for Information Technologies in Education

8 Kedrova St. (Bldg. 3), 117292 Moscow, Russian Federation

The designations employed and the presentation of material throughout this publication do not imply the expression of any opinion whatsoever on the part of UNESCO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The ideas and opinions expressed in this publication are those of the authors; they are not necessarily those of UNESCO and do not commit the Organization.

Cover photo: © Data Protection and Privacy by Cerillion, CC BY 2.0

Contents

Preface

Personal data security in education has been a long-standing issue with development of online learning. However, it has never been so critical as today during the COVID-19 pandemic and prioritized by UNESCO among the top challenges we are confronting. Therefore, technical recommendations on personal data security for online education platforms are urgently needed both for current situation and for long term education planning. The UNESCO Institute for Information Technologies in Education (UNESCO IITE) in partnership with the research team led by Professor Xiaoyun Wang at Tsinghua University has drafted this technical guide. Professors from Shanghai Jiaotong University, Shandong University and technical experts from Microsoft, Alibaba, Tencent, Inspur and Blackboard have made collective contribution to the accomplishment of this work in a short period of time.

The aim of this Technical Guide is to outline key recommendations to online education platform providers and relevant education and technical administrators in terms of technical solutions, management as well as awareness raising. It has been drafted following the basic principles of the United Nations (UN) for personal data protection, documents adopted by relevant UN Agencies such as UNICEF, UNDG and ITU as well as technical ISO standards. Technical specifications and regulations from other international organizations and different countries and regions are also referred. In addition, thanks to the research teams and experts engaged, this Technical Guide reflects the most advanced technologies in data security and protection.

Tao Zhan

Dr Tao Zhan

Director

UNESCO Institute for Information Technologies in Education (IITE)

Xiaoyun Wang

Professor Xiaoyun Wang

Institute of Advanced Study

Tsinghua University, China

1 Introduction

1.1 Background and Rationale

While digital technology is evolving rapidly and bringing more and more people and innovations to online teaching and learning, personal data security of students and teachers becomes a major concern and one of the most challenging issues of online education. However, this issue has never been so critical and urgent as it is during the current COVID-19 pandemic, when online learning is the only plausible solution wherever the Internet is available.

With school and university closures to contain the spread of COVID-19, addressing the immediate educational consequences requires emergency measures at all levels. Nations adapt innovative and flexible ways to facilitate teaching and learning through different channels and media. Thanks to advanced information and communication technologies, millions of students are keeping up with their learnings during this tough time. However, without solid data security guidelines, both in terms of technology and management, such unprecedented switch might generate great threats to privacy and protection of personal data, both for students and teachers. It is therefore necessary to develop a common approach to the use of online education platforms, which is supported by universally recognized personal data security principles as well as by trusted technology and concise regulations that enable the accountable use of personal data in the public interest.

Personal data privacy and protection is part of human rights as declared in the Resolution 68/167 adopted by the United Nations (UN) General Assembly, which emphasizes “unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression”. In this context, personal data of school students, most of whom are children, demand particular attention and more accurate measures. More and more countries and regions are adopting comprehensive regulations on personal data privacy and protection with regard to students and teachers.

During the COVID-19 pandemic, UN and its agencies, including UNESCO, stand ready to help facilitate the swift and safe switch to online education. In this global approach, personal data privacy and protection will remain among the top issues, not only as a pressing challenge during the crisis but also as a vital part of long-term strategy for developing more resilient education systems.

1.2 Goal and Scope

The overarching goal of this Technical Guide is to promote the rights to privacy of teachers and students of all ages and protection of their personal data. It aims to provide technical recommendations for service providers of online education platforms that are compliant with universally acknowledged security principles and advanced data security technologies, to help improve overall security of online education platforms in personal data management and protection.

This Technical Guide is designed for service providers of online education platforms and educational stakeholders to minimize the risks while managing personal data of students and teachers. Additionally, beyond providing the front-line support to individuals and communities during the COVID-19 outbreak, it will assist educational authorities to ensure the personal data security in online education with respect to national and international regulations.

Online education platforms differ largely both in terms of technologies they built upon, and in terms of their functionality to support teaching and learning. This Technical Guide intends to cover the commonly used online education platforms which are open to schools, universities and individual learners. Since special requirements are needed for personal data security of online Education Management Information Systems (EMIS), they are not included in this Technical Guide due to the scope of their data collection and management functions.

This Technical Guide follows general principles adopted by the UN General Assembly and the UN High-Level Commission on management of personal data privacy and protection. Official documents issued by UNICEF, ITU, ISO/IEC and other relevant organizations as well as regulations at country and regional levels are referenced in this Technical Guide.

2 Terminology and Definition

For the purposes of this document, the terms and definitions that are given in ISO/IEC 27000, ISO/IEC 29100 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org

2.1 Personal Data in Online Education Platforms

The data collected by online education platforms consists primarily of personal data, which is mainly collected from students, their guardians and teachers.

a) PERSONAL DATA: the information that relates to an identified or identifiable individual.

b) STUDENT'S PERSONAL DATA: the information that relates to a specific student, including students' personally identifiable information (PII), contact information such as school, grade, class, and home address, learning behavior information such as academic performance, test scores, student files, and platform access information, etc.

c) GUARDIAN'S PERSONAL DATA: the information that relates to the guardian of a student, including his or her PII, relevant information about related students, and platform access information, etc.

d) TEACHER'S PERSONAL DATA: the information that relates to the teachers of the platform, including his or her PII, contact information such as position, school, grade, class, and home address, teaching information such as courses taught, courseware, knowledge points, and platform access information, etc.

2.2 Data Lifecycle

The complete data lifecycle defined in this guide includes the following five stages: collection, transmission, usage, storage, and destruction.

2.3 Security Properties and Measures

This guide mainly concerns with the following security properties and measures of personal data.

a) CONFIDENTIALITY: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC 27000:2018, Definition 3.10]

b) INTEGRITY: Property whereby data have not been altered in an unauthorized manner since they were created, transmitted or stored. [ISO/IEC 29167-19:2019, Definition 3.3]

c) AVAILABILITY: Property of being accessible and usable upon demand by an authorized entity. [ISO/IEC 27000:2018, Definition 3.7]

d) AUTHENTICITY: Property that an entity is what it claims to be, which can be achieved by means of password, digital signature, biometrics and multi-factor authentication, etc. [ISO/IEC 27000:2018, Definition 3.6]

e) NON-REPUDIATION: Ability to prove the occurrence of a claimed event or action and its originating entities. [ISO/IEC 27000:2018, Definition 3.48]

f) ACCESS CONTROL: Means to ensure that access to assets is authorized and restricted based on business and security requirements. [ISO/IEC 27000:2018, Definition 3.1]

2.4 Cryptographic Primitives

This guide refers to the following cryptographic algorithms for protecting personal data.

a) ENCRYPTION ALGORITHM: Process which transforms plaintext into ciphertext to protect the confidentiality of data. [ISO/IEC 18033-1:2015, Definition 2.22]

b) HASH FUNCTION: Function which maps arbitrary-length message into a fixed-length output called a digest satisfying preimage attack resistance, second preimage attack resistance and collision resistance. Hash functions are typically used to prevent messages from being tampered with and therefore ensure the integrity of messages.

c) DIGITAL SIGNATURE: The signer uses his or her private key to cryptographically transform the message into a fixed-length bit string called a digital signature. The digital signature can be publicly verified by others, but it is computationally infeasible for others to forge a valid signature. Digital signature is used to protect the integrity of the message, the authenticity of the signer's identity and the non-repudiation of the signing behavior.

d) MESSAGE AUTHENTICATION CODE: The sender uses his or her key to perform cryptographic transformation on the message to generate a fixed-length bit string, called a MAC tag in short. Any recipient who shares the same key can verify the correctness of the MAC tag, but it is infeasible for those not in possession of the key to forge the MAC tag, which ensures the integrity of the message.

3 Personal Data Risks Overview for Online Education Platforms

Online education platforms are essential to online education activities. Different online education platforms serve their specific educational scenarios and may vary in characteristics and advantages. With the advance of the globalization of online education, the privacy and protection of personal data on online education platforms has increasingly become a major concern. This chapter first introduces several types of representative online education platforms and their associated personal data, and then gives an overview of security risks and threats of personal data on online education platforms.

3.1 Overview of Online Education Platforms

Online education is an educational approach based on the Internet context. Educational resources, activities, presentations and other components of this approach are all delivered or organized over the Internet. Its implementation has to be supported with a technology-enriched environment, the so-called online education platform, and its application to maintain various online learning settings and conduct diverse online learning activities. Based on the real practical online learning scenarios, currently online education platforms can be categorized as the following four types. The personal data security issues are also embodied accordingly, including data categories and their roles in online education.

3.1.1 Webcasting

Webcasting is the combination of the words “web” and “broadcast”. A webcast is a live or on-demand media presentation broadcasted over the Internet. Teachers can use webcasting to deliver learning contents, such as presentation, demonstration, or interpretation. Webcasting is widely used by schools, universities and for online training. Its usage normally assumes personal data of schools, universities and training institutions, such as registration IDs including personal accounts and PINs, personal information, lists of participants, video scripts, and other relevant information upon requirement.

3.1.2 Online Learning Management Systems (OLMS)

OLMS provides educators with an integrated learning environment with broad functionality to manage courses, track students learning records and maintain online discussions. Compared with other online education platforms, OLMS is a formal, closed, integral, and well-functioned system which has played an important role in supporting online learning. There are many examples of OLMS with an open license or a limited access with license-control. OLMS is usually a data-rich environment where there are plentiful learning and teaching data produced by students and teachers alone with each online learning session. It is very important to secure personal data collected or produced from students and teachers, including personal information, learning contents, discussion scripts, learning records, and performance data etc.

3.1.3 Massive Open Online Course (MOOC) Platforms

In the past decade, MOOCs have become popular and widely used in many universities and colleges. The specific MOOC platforms bring lots of conveniences to students and teachers to register in and manage their learning and teaching process. MOOC platforms are mainly used for university students or adult learners. When a MOOC course has been selected for online learning, one needs to register in a MOOC platform. In this context, logged personal data typically contains the basic personal information and track records.

3.1.4 Communication Tool

Communication tools are also widely used in various online learning scenarios to support instant communication between teachers and students, or students and students. There are many kinds of communication tools based on text, audio, or video formats. Communication tools are typically used as connection facilities, like mobile handsets the provide anyone, anytime, and anywhere with a way to communicate. It could empower online education, as it is especially effective and efficient if supported by instant communication. Notifications, search, feedback, reinforcement, or assignments can be delivered by communication tools. Therefore, personal data related to those activities would be taken into consideration for online learning.

3.2 Security Risks of Personal Data in Online Education Platforms

The online education platform may carry various risks and threats associated with the employed technologies, process management and user operations. These may cause security issues such as thefts and integrity violations of personal data, unauthorized data destruction, and impersonation fraud, which further brings reputational damage, mental injury and financial loss to platform users. Personal data related to online education platforms mainly faces security risks of the following three aspects.

3.2.1 Technical Risk

Due to the insufficiency or incompetence of security technologies, and misuse of cryptographic and network security technologies for platform protection, there may be system vulnerabilities, software and hardware vulnerabilities, and network vulnerabilities that can be exploited by attackers. This further leads to data thefts, system intrusions and access control breaches, and eventually compromises the security of the user’s personal data.

3.2.2 Management Risk

Due to the lack of security awareness, platform operations managers may collect user personal data without consent or exceeding preauthorization, fail to protect the life cycle of data, unreasonably allocate access rights to users, deploy platform resources or load configurations, fail to maintain platform resources and databases on a regular basis, fail to patch the systems and update their virus database in time. They may not have proper disaster recovery or data backup measures in place, disclose and share users' data without authorization, etc.

3.2.3 User Operational Risk

Users who lack security awareness might use weak passwords, fail to properly protect passwords, biometrics and OTP devices and other authentication methods, allow a platform to collect personal data without authorization or beyond necessary, install their client platform in an untrustworthy computing environment, fail to properly configure the access rights of their personal data, and fail to implement necessary protection, backup or destruction measures for personal data.

4 Principles of Personal Data Protection

The “Principles” adopted by UN HLCM (UN High-level Committee on Management) set out a basic framework for the processing of “personal data”. These principles aim to harmonize standards for the protection of personal data in online education platforms, facilitate the accountable processing of personal data for specific and legitimate purpose and ensure respect for the human rights and fundamental freedom of individuals, in particular the right to privacy.

a) FAIR AND LEGITIMATE PROCESSING: The Online Education Platform should process personal data in a fair manner, in accordance with the applicable international and regional mandates and governing instruments and on the basis of any of the following: (i) the consent of the data subject; (ii) the best interests of the data subject, consistent with the mandates of the United Nations and educational industry concerned; (iii) 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; or (iv) any other legal basis specifically identified by international or regional laws, regulations and contractual clauses.

b) PURPOSE SPECIFICATION: Personal data should be processed for specified purposes, which are consistent with the mandates of the Online Education Platform operators concerned and take into account the balancing of relevant rights, freedoms and interests. Personal data should not be processed in ways that are incompatible with such purposes.

c) PROPORTIONALITY AND NECESSITY: The processing of personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing.

d) RETENTION: Personal data should only be retained for the time that is necessary for the specified purposes.

e) ACCURACY: Personal data should be accurate and, where necessary, up to date to fulfill the specified purposes.

f) CONFIDENTIALITY: Personal data should be processed with due regard to confidentiality.

g) SECURITY: Appropriate organizational, administrative, physical and technical safeguards and procedures should be implemented to protect the security of personal data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.

h) TRANSPARENCY: Processing of personal data should be carried out with transparency to the data subjects, as appropriate and whenever possible. This should include, for example, provision of information about the processing of their personal data as well as information on how to request access, verification, rectification, and/or deletion of that personal data, insofar as the specified purpose for which personal data is processed is not frustrated.

i) TRANSFERS: In carrying out its mandated activities, an Online Education Platform may transfer personal data to a third party, provided that, under the circumstances, the Online Education Platform operator satisfies itself that the third party affords appropriate protection for the personal data.

j) ACCOUNTABILITY: The Online Education Platform operators should have adequate policies and mechanisms in place to adhere to these Principles.

5 Recommended Technical Solutions

This chapter suggests relevant data security protection technologies that online education platforms should take from the aspects of data lifecycle security, network and system security, cryptography technology and key management.

5.1 Security of Data Lifecycle

5.1.1 Data Collection

The data collection performed by the online education platform should comply with the security principles, and providing classification and category of the data according to data attributes such as of types, sensitivities. The online education platform should have the consent or authorization of a guardian when collecting and using information of juveniles. When data is marked as PII or information related to a PII body, the online education platform should implement privacy security controls.

5.1.2 Data Transmission

To ensure data transmission security, the online education platform should establish an appropriate protection mechanism in the process of data transmission, and use network security protocols such as TLS, IPSec, etc., and use cryptography algorithms recommended by the relevant standards.

5.1.3 Data Usage

Online education platforms should provide unified rights management to ensure that users apply and access relevant data on demand in accordance with the principle of least privilege. The online education platform should provide comprehensive security monitoring and access auditing measures for the use and access of relevant data, as well as PII protection mechanisms (including but not limited to privacy protection technologies such as de-identification and pseudo-anonymization technologies).

5.1.4 Data Storage

The online education platform's data storage should comply with the security principles and be protected by access control and security protection to prevent unauthorized access, modification, destruction, removal, or other use. Such mechanisms include, but are not limited to, encryption, signature, anonymization, key management, etc.

The online education platform should have the capabilities of high availability, data backup and disaster recovery to ensure reliability and availability of the data.

5.1.5 Data Destruction

The online education platform should destroy the data according to the data classification and storage media. Before information processing facilities and storage media are removed from the online education platform, data removal and physical destruction should be carried out in accordance with relevant standards to avoid the risk of data leakage.

5.2 Network and System Security

5.2.1 Communication Network

The online education platform should refer to the relevant standards, adopt the reasonable security design and deployment for access control and application development. Deploy the security control measures or security services such as link redundancy, network intrusion detection, network anti-virus, network security audit, authentication, encryption, intrusion detection to protect the network transmission security.

5.2.2 Computing Environment

The online education platform should refer to the relevant standards, and have the ability to protect, monitor and audit the computing environment such as operating system, database, middleware, etc., to ensure the security of the platform computing environment.

5.2.3 Access Control

Applications of the online education platform should refer to the relevant technical standards to take technical measures to achieve access control in the aspects of user account management, authentication, rights management, behavior audit, etc.

5.3 Cryptographic Techniques and Key Management

5.3.1 Cryptographic Algorithms and Protocols

The online education platform should adopt the cryptographic algorithms and protocols recommended by the cryptographic standards currently effective or be with provable security, and meet the requirements of key strength.

5.3.2 Key Management

The online education platform should strictly manage the keys to ensure the security throughout the keys' lifecycle. The key's lifecycle includes generation, storage, distribution, import, export, use, backup, recovery, archiving, and destruction. Key management technical requirements can refer to ISO/IEC 11770.

6 Recommended Security Management

Data has its inherent life cycle, from creation, generation, storage, processing, using, transmission, to the eventual destruction or disappearance, for which the security gained merely through technical means is limited and should be supported through appropriate management and regulations. Data security management should be based on ISO/IEC27001 Information Security Management System (ISMS) and ISO/IEC27701 Privacy Information Management System (PIMS), and be a part of the overall management system of the organization, which mainly includes organizational environment, strategy formulation, risk assessment, risk control, security incident monitoring and handling, etc.

6.1 Security Management Planning

6.1.1 Security Management Policies

The online education platform shall define the scope and boundaries of security management, develop the enterprise's security management policies and guidelines, including personal data security, as well as related physical security, data security, device security, security configuration, network security, application security, data backup and disaster recovery, etc.

Personal data security guidelines and security objectives shall be consistent with the organization's strategy orientation.

The education platform shall comply with territorial laws and regulations and protect users' personal data, and shall establish data sharing and disclosure policies and mechanisms if the education platform needs to share and disclose user personal data to the external, to ensure that data receiver meets relevant privacy protection requirements and have equal or appropriate personal data protection capabilities.

6.1.2 Security Management Organization

The online education platform shall establish a sound security organization structure, clarify security-related positions and responsibilities, and should set up dedicated data security functional departments and positions, and separate the roles in key positions.

The top management of education platforms shall ensure that the resources required for the security management of personal data are available.

Education platforms shall organize training to ensure that employees have necessary skills and security awareness of personal data protection principles.

6.1.3 Risk Assessment

The online education platforms should identify risk assessment and risk criteria, as well as risk treatment plans after security technology control measures covered in chapter 6 are implemented. Referring to the risks described in Chapter 4 to analyze internal vulnerabilities and external threats, and determine the levels of risks after analysis is advisable. Additionally, it is recommended to identify further risks based on a developed risk treatment plan and risk criteria, and outline a risk control implementation plan.

6.2 Security Monitoring and Audit

6.2.1 Security Incident Monitoring

Relevant international standards shall be referred to draw up security incident monitoring programs, and to carry out regular and effective security monitoring in accordance with the plan. Be capable of informing security incidents, perceiving security situation, and establish a mechanism for disclosure and handling of security vulnerabilities. There should be public disclosure and a communication plan based on an impact level of security incident.

6.2.2 Security Incident Audit

The platform shall be able to audit critical security incidents, with granular audits covering both users and a system, and have audit trails and traceability. The platform also shall have capability to read, restore, analyze the audit log, identify the root cause or investigate security incident when needed.

6.3 Security Incident Response and Disposition

6.3.1 Security Incident Response

The network security incident emergency plan and emergency response procedures shall be developed to determine the reporting process of an incident, the scope and extent of the response and the disposal methods. In the event of an incident that endangers the network security, immediately initiate emergency plan and take appropriate remedial measures.

6.3.2 Security Incident Disposition

When network and information security incidents occur, measures shall be taken in time to control the situation. In the process of disposition, it is necessary to analyze and identify causes of the incident, document the disposal process, learn lessons, develop remedial measures to prevent recurrence. All documented information shall be properly preserved.

7 Awareness Raising of Personal Data Privacy and Protection

As efficient counter-measures require more than just regulatory activities related to service providers and education administrators, it is advisory to further strengthen education for personal data privacy and protection of students and teachers in order to improve personal awareness and behavior as the part of future digital society and culture.

7.1 Promotion through Curriculum in Formal Education

Through primers, exercises and further discussions children can become familiar with essentials for personal data privacy and protection and unconsciously accept them as a rule of thumb during their years at school. Thus, a structured school environment and teaching workforce equipped with purposefully designed curriculum activities can become the front-line support to the society and ensure the safety in online education.

7.2 Promotion within Digital Citizenship Education

Digital citizenship is an evolving concept encompassing key competencies and values, i.e. a set of vital skills that everyone needs to acquire for appropriate interaction with information and other digital citizens online. By turning classrooms into a training ground for digital citizenship, teachers can prepare their students to use the Internet safely, review the content critically and accomplish their goals.

It is important to equip users of all ages with knowledge about digital citizenship, including the knowledge of the right for personal data privacy and protection, as this is a one of the key elements of digital literacy. Additionally, incorporating relevant activities into standard curriculum subjects is recommended as the first step towards integrating the youth into digital societies and engage them in the work towards the achievement of Sustainable Development Goal 4.

7.3 Promotion through Public Engagement

As online education platforms can reach a broad range of individuals across society, open online courses can become one of the main entry points for popularizing knowledge of human rights, particularly the right for personal data privacy and protection. However, disseminating educational materials on ongoing and planned initiatives on the matter, including this Technical Guide, through all available media channels and further activities within awareness raising campaigns will highlight best practices and eventually lead to a higher level of security culture in the society.

8 References

1. UN (2014). A/RES/68/167. The right to privacy in the digital age. Retrieved May 14, 2020 from https://undocs.org/A/RES/68/167
2. UNDG (2017). Data privacy, ethics and protection: Guidance note on big data for achievement of the 2030 agenda. Retrieved May 14, 2020 from https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf
3. UN HLCM (2018). Personal data protection and privacy principles. Retrieved May 14, 2020 from https://www.unsceb.org/CEBPublicFiles/UN-Principles-on-Personal-Data-Protection-Privacy-2018.pdf
4. UNICEF (2018). Children’s Online Privacy and Freedom of Expression: Industry Toolkit. Retrieved May 14, 2020 from https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf
5. UNICEF (2020)— Technical note: COVID-19 and its implications for protecting children online. Retrieved May 14, 2020 from https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf
6. ITU / UNICEF (2015). Guidelines for Industry on Child Online Protection. Retrieved May 14, 2020 from https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf
7. ITU (2009). Guidelines for Policy Makers on Child Online Protection. Retrieved May 14, 2020 from https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf
8. ISO/IEC 27001:2019 Information technology — Security techniques — Information security management systems — Requirements.
9. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.
10. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.
11. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines.
12. ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework.
13. ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment.
14. ISO/IEC 29151:2017 | ITU-T X.1058 Information technology — Security techniques — Code of practice for personally identifiable information protection.
15. ISO/IEC 29187-1:2013 Information technology — Identification of privacy protection requirements pertaining to learning, education and training (LET) — Part 1: Framework and reference model.
16. ISO/IEC 27000:2018 Information technology — Security techniques —

Information security management systems — Overview and vocabulary

17. ISO/IEC 27040:2015 Information technology — Security techniques — Storage security.
18. ISO/IEC 18033-3:2010 Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers.
19. ISO/IEC 18033-2:2006 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers.
20. ISO/IEC 10118-3:2018 IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions.
21. ISO/IEC 15946-2:2002 Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures.
22. ISO/IEC 11770:2008 Information technology — Security techniques — Key management.
23. The European Parliament and the Council (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved May 14, 2020 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
24. OECD (2012). The Protection of Children Online. Retrieved May 14, 2020 from https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf