unesco

Minding the data

Protecting learners' privacy and security

Education 2030

UNESCO – a global leader in education

Education is UNESCO’s top priority because it is a basic human right and the foundation for peace and sustainable development. UNESCO is the United Nations’ specialized agency for education, providing global and regional leadership to drive progress, strengthening the resilience and capacity of national systems to serve all learners. UNESCO also leads efforts to respond to contemporary global challenges through transformative learning, with special focus on gender equality and Africa across all actions.

The Global Education 2030 Agenda

UNESCO, as the United Nations’ specialized agency for education, is entrusted to lead and coordinate the Education 2030 Agenda, which is part of a global movement to eradicate poverty through 17 Sustainable Development Goals by 2030. Education, essential to achieve all of these goals, has its own dedicated Goal 4, which aims to ***“ensure inclusive and equitable quality education and promote lifelong learning opportunities for all.”*** The Education 2030 Framework for Action provides guidance for the implementation of this ambitious goal and commitments.

unesco

United Nations
Educational, Scientific
and Cultural Organization

Education 2030

Published in 2022 by the United Nations Educational, Scientific and Cultural Organization,
7, place de Fontenoy, 75352 Paris 07 SP, France

ISBN 978-92-3-100525-1
https://doi.org/10.54675/NNAA4843

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: HQuality/Shutterstock.com

Designed and printed by UNESCO

Printed in France

SHORT SUMMARY

Protecting learners' privacy and security

The COVID-19 pandemic greatly accelerated the use of digital technologies in education. But beyond the emergency response, there is an international trend towards exploring how artificial intelligence and data-based analytics can support learning, learning assessments, and evidence-based policy planning processes.

The use of data in education is a double-edged sword. On the one hand, they offer tremendous potential to create value by improving policies and programmes, driving transparent governance and better management of education systems, teachers' empowerment, personalized learning experiences, assessment, and certification. On the other hand, data accumulation can lead to a concentration of economic and political power, raising the possibility that data may be misused in ways that harm learners.

This publication argues that a balance must be struck between the use of technology to advance educational transformation and the safeguarding of privacy and individual rights. Proper rules and protocols are needed to protect students and teachers not only in national policies but also at international level, where cooperation and collaborative efforts are also required to support policy learning, knowledge sharing and mutual understanding.

UNESCO launches through this publication a clarion call to the education community not only to pay careful attention to data privacy in education, but to take the lead in these developments.

The use of **data in education is a double-edged sword**

UNESCO

"Since wars begin in the minds of men and women it is in the minds of men and women that the defences of peace must be constructed"

Minding the data

Protecting learners' privacy and security

Acknowledgments

This publication was written by (in alphabetical order) Borhene Chakroun, Director of UNESCO's Division for Policies and Lifelong Learning Systems, Katrien Daelman-Balepa, International Consultant, and James Keevy, CEO of JET Education Services, with support from Elise Rondin, Division for Policies and Lifelong Learning Systems and contribution from Katherine Morris, Research associate at JET Education Services.

The authors wish to acknowledge the following UNESCO experts who have contributed to this publication (in alphabetical order): Gwang-Chol Chang, Huong Le Thu, Rolla Moumné, Mark West and Satoko Yano.

The following reviewers also provided valuable contributions: Experts from the Commission Nationale Informatique et Libertés (France), especially Marie Heuzé, Délia Rahal-Löfskog, Pascale Raulin-Serrier and Elodie Weil; Guy Huntington, Legal Self-Sovereign Identity (LSSI) Specialist, Huntington Ventures Ltd, Mariagrazia Squicciarini and Saurabh Roy, of UNESCO's Social and Human Sciences Sector.

Borhene Chakroun managed the coordination of the drafting process and Rolla Moumné and Elise Rondin coordinated the production and publication process.

Table of contents

List of boxes

List of tables

Glossary of terms related to data privacy in education

This glossary provides illustrative definitions to facilitate the reading of the document. These illustrative definitions do not imply the expression of any opinion whatsoever on the part of UNESCO.

Term	Illustrative definition and main sources
Anonymization	'[I]information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.' https://gdpr.eu/article-4-definitions/
Application Programming Interface (API)	'[A] set of defined rules that explain how computers or applications communicate with one another. APIs sit between an application and the web server, acting as an intermediary layer that processes data transfer between systems'. https://www.ibm.com/cloud/learn/api
Artificial intelligence	'[T}echnological systems which have the capacity to process information in a way that resembles intelligent behaviour, and typically includes aspects of reasoning, learning, perception, prediction, planning or control'. https://unesdoc.unesco.org/ark:/48223/pf0000373434
Cloud-based computing	'[O]n-demand access, via the internet', to remotely hosted computing resources such as applications, servers, data storage and networking capabilities. https://www.ibm.com/za-en/cloud/learn/cloud-computing
Consent	'Any freely given, specific, informed and unambiguous indication' by an individual signifying 'agreement to the processing of their personal data'. https://gdpr.eu/gdpr-consent-requirements/
Credential fluency	The increasingly seamless interrelationships between the recognition of formal, non-formal and informal lifelong learning made possible through a user-centric approach, digital forms of recognition, improved data interoperability, and closer alignment between learning and the world of work. https://www.purdue.edu/hhs/psy/tmag/
Cybersecurity	The 'systems and actions aimed at securing data and communications over the internet'. http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide
Data analytics	The systematic and scientific processing and analysis of data or statistics, and the information resulting from that analysis. https://www.lexico.com/definition/Analytics
Data breach	The intentional or accidental 'destruction, loss, alteration, unauthorized disclosure of, or access to, personal data'. https://gdpr.eu/article-4-definitions/
Data broker	An individual or company that collects and sells personal data to third parties for various purposes. https://doi.org/10.1787/5k486qtxldmq-en
Data controller/ data fiduciary	A 'natural or legal person, public authority, service, agency, or any other body which, alone or jointly with others, has decision-making power with respect to data processing'. The term 'data fiduciary' was introduced in India's Personal Data Protection Bill (2018) and is equivalent to the GDPR's conceptualization of a 'data controller', although the use of 'fiduciary' implies that the relationship involves a measure of trust. https://rm.coe.int/16808ade9d
Data disclosure	The 'transmission, dissemination or otherwise making available' of data to an authorized or unauthorized party. https://gdpr.eu/article-4-definitions/

Term	Illustrative definition and main sources
Data ecosystem	The complex web of organizations and individuals which directly and indirectly consume, generate, share and process data and related resources, including software, services and infrastructure. https://doi.org/10.1145/3209281.3209335 https://dl.acm.org/doi/abs/10.1145/3209281.3209335
Data lake	'A data lake is a centralized repository designed to store, process, and secure large amounts of structured, semi-structured, and unstructured data. It can store data in its native format and process any variety of it, ignoring size limits.' https://cloud.google.com/learn/what-is-a-data-lake
Data mining	The exploration and analysis of large amounts of data in order to derive new information or knowledge from that data. https://doi.org/10.1007/978-1-4419-9863-7_599
Data privacy	The rights that empower 'users to make their own decisions about who can process their data and for what purpose'. Such rights include, for example, the right to be informed or the rights of access, rectification, and erasure. https://gdpr.eu/data-privacy/
Data processing	'[A]ny operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data'. https://rm.coe.int/16808ade9d
Data processor	'[A] natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'. https://gdpr.eu/data-privacy/
Data protection	The responsible use of personal data by ensuring that data is used fairly, lawfully and transparently, for specified, explicit purposes in a way that is relevant and limited only to what is necessary. Data should be kept for no longer than is necessary and handled in a way that ensures appropriate data security. https://gdpr.eu/article-5-how-to-process-personal-data/
Data protection officer	A person responsible for overseeing an organization's data protection strategy, implementation, and compliance. https://gdpr.eu/data-protection-officer-responsiblities/
Data security	The securing of personal and other kinds of data against 'unauthorized or unlawful processing, loss, theft, destruction, or damage'. http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide
Data subject	Any person who is identified or identifiable through personal data. https://gdpr.eu/article-4-definitions/
Data-driven decision-making	Using data to inform decisions and implement change. In an educational context, 'data' can include, for example, information about the student, classroom or school that can be analysed such as behavioural data, biometric data, learning assessment data and learning interaction data. https://dx.doi.org/10.4135/9781506326139.n183
Datafication	The process of quantifying elements of human life into forms of digital information so that they can be measured, tabulated and analysed, and used as a continuous source of data). https://policyreview.info/concepts/datafication
Digital credential	A digital record of focused learning achievement verifying what the learner knows, understands and/or can do. https://europa.eu/europass/en/what-are-digital-credentials
Digital literacy	'An individual's ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital technologies.' http://uis.unesco.org/en/blog/global-framework-measure-digital-literacy

Term	Illustrative definition and main sources
Digital pedagogies	How best to use existing, new and emergent digital technologies in teaching and learning. https://www.jisc.ac.uk/full-guide/digital-pedagogy-toolkit)
Digital skills	The skills required to use digital technology in daily life. These skills 'are best understood on a graduated continuum from basic functional skills to higher-level, specialist skills' and include 'a combination of behaviours, expertise, know-how, work habits, character traits, dispositions and critical understandings'. https://unesdoc.unesco.org/ark:/48223/pf0000259013
Digital twin	'[A] virtual representation of an object or system that spans its lifecycle, is updated from real-time data, and uses simulation, machine learning and reasoning to help decision-making'. https://www.ibm.com/topics/what-is-a-digital-twin
Digitization	Process of converting analogue information into a digital format. https://www.gartner.com/en/information-technology/glossary/digitization
Education Management Information System (EMIS)	A 'system for the collection, integration, processing, maintenance and dissemination of data and information to support decision-making, policy analysis and formulation, planning, monitoring and management at all levels of an education system. It ... [aims] to provide education leaders, decisionmakers and managers at all levels with a comprehensive, integrated set of relevant, reliable, unambiguous and timely data and information to support them in completion of their responsibilities'. https://publications.iadb.org/en/publication/education-management-information-systems-emis-latin-america-and-caribbean-lessons-and
Inferred data	'Inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject"'. https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
Information flow	The movement of data or information from one location to another. This includes information flow between companies or organizations, nationally or internationally. https://www.itgovernance.co.uk/gdpr-data-mapping
Internet of Things (IoT)	'[A] system involving connected devices that gather data, connect with the Internet or local networks, generate analytics, and (in some cases) adapt behaviour/responses based on the data/analytics in the network'. https://openknowledge.worldbank.org/handle/10986/28661
Interoperability	'[T]he ability of discrete computer systems or software to exchange and make meaningful use of shared data or other resources.' https://www.jet.org.za/resources/interoperable-data-ecosystems.pdf
Learning management system (LMS)	'[LMS] integrate interactive learning environments and administration and facilitate customized online instructional materials. An LMS is a web-based software application using a database on which various types of information are stored'. https://doi.org/10.1007/978-1-4419-1428-6
Massive Online Open Courses (MOOCs)	'Online courses designed for a large number of participants that can be accessed by anyone anywhere, as long as they have an internet connection.' https://publications.jrc.ec.europa.eu/repository/handle/JRC96968
Notice-and-choice regimes	A means for 'websites or other online services [to] provide individuals with disclosure about their information practices, such as those pertaining to data collection, use, sharing, and security.' https://ir.lawnet.fordham.edu/iplj/vol27/iss1/5
Open data	Data that can be freely used, re-used and distributed without restriction. https://opendefinition.org/

Term	Illustrative definition and main sources
Open educational resources	'[T]eaching, learning and research materials in any medium - digital or otherwise - that reside in the public domain or have been released under an open license that permits no-cost access, use, adaptation and redistribution by others with no or limited restrictions.' https://unesdoc.unesco.org/ark:/48223/pf0000246687?posInSet=1&queryId=10fe2a4e-db8c-4213-94d5-c05deb855ec9.
Personal data	'[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'. https://gdpr.eu/article-4-definitions/ Also see: https://globalprivacyassembly.org/wp-content/uploads/2021/10/1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf
Privacy-Enhancing Technologies (PETs)	A wide range of 'technologies that support privacy or data protection features'. https://www.enisa.europa.eu/publications/pets
Processing	'[A]ny operation or set of operations carried out or not, with the assistance of processes that may or may not be automated, and applied to data, such as obtaining, using, recording, organization, preservation, adaptation, alteration, retrieval, saving, copying, consultation, utilisation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, encryption, erasure or destruction of personal data'. https://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf
Profiling	'[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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'. https://gdpr.eu/article-4-definitions/
Recipient	'[A] natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available'. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
Self-sovereign identity	'[T]he digital movement that recognizes an individual should own and control their identity without the intervention of administrative authorities', allowing an individual full control over their digital persona. https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignity-digital-wallets-and-blockchain
Sensitive data	'1.a. Data which affect the data subject's most intimate sphere; or b. Data likely to give rise, in case of misuse, to: i. Unlawful or arbitrary discrimination; or ii. A serious risk to the data subject.' https://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf
Technology-enhanced learning	The use of technology such as film, radio, television, computers and smart devices to support face-to-face and remote learning. https://link.springer.com/referenceworkentry/10.1007%2F978-3-319-60013-0_72-1
Third party	'[A]ny public or private individual or legal entity, body or association other than the data subject, the data controller, the data processor and any other persons placed under the direct authority of the data controller or the data processor, who is authorised to process data.' https://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf
Transparency Principle	The person responsible shall inform the holder about the existence and main characteristics of the treatment to which their personal data will be subjected, so they can make informed decisions about it. https://platform.dataguidance.com/sites/default/files/02.24.20_ibero-am_standards.pdf

Executive summary

The growth of data, their socio-economic implications and their integration into the lives and work of most people everywhere are spurring the data revolution. Industry 4.0 is transforming manufacturing industry into a new paradigm, in particular with regard to data ecosystems and potential. Social sectors such as education, health and social security are following suit.

The education sector is no stranger to the digital movement. The Education 2030 Framework for Action (UNESCO, 2015) provides guidance for the implementation of the Education 2030 Agenda and highlights how the focus on lifelong learning and the provision of broad and flexible pathways requires ICTs to complement and supplement formal schooling. The Qingdao Declaration addresses a variety of ways in which ICTs and increased connectivity can be leveraged to achieve the Education 2030 Agenda and open up new opportunities for lifelong learning. More recently, the Beijing Consensus on artificial intelligence and education considers the potential ways in which artificial intelligence (AI) can profoundly transform education and lifelong learning systems, and aims to frame an appropriate policy response.

The COVID-19 pandemic and the migration of education systems to remote and digital learning has accelerated the use of digital technologies in education. In addition to the emergency response, there is an international trend to explore how AI and data-based analytics can support learning, learning assessments and evidence-based policy planning processes. This has driven improvements in personalized, adaptive and flexible learning processes and pathways, an enhanced ability to evaluate the multiple dimensions of learners' competencies, and better-informed education management systems.

This trend has two effects. The first is the need for large data sets drawn from aggregation of learning profiles, micro-behaviours, access time and Online. See page actions, to build patterns and better understand learning processes, effectiveness and problems.[1] The second is a change in approach to the concept of privacy and security. Data are seen as essential for education, an indispensable tool for individualized learning processes, reliable information about access to learning opportunities, tracking progress and assessing learning outcomes and beyond, in terms of labour market and social outcomes (OECD, 2012b; UNESCO, 2021).

The ease of data capture, storage, processing and monitoring in digital learning spaces has spurred applications and growth. However, the use of data in education is a double-edged sword. On the one hand, they offer tremendous potential to create value by improving policies and programmes, driving transparent governance and better management of education systems, teachers' empowerment, personalized learning experiences, assessment and certifications. On the other hand, data accumulation can lead to a concentration of economic and political power, raising the possibility that data may be misused in ways that harm learners. During the pandemic, education systems placed unprecedented reliance on private technology providers as they worked to ensure the continuation of education and learning during prolonged periods of school closure. Hence, a balance must be struck between the use of technology to advance education transformation and the safeguarding of privacy and individual rights.

The gaps in data protection, privacy, ownership, governance and security – with specific reference to learners – are part of the broader digital divide. While the digital divide is usually measured in differences within and across countries in areas such as digital literacy, access to bandwidth, use of sophisticated devices, platforms and education resources, the lack of legislation specifically relating to learners' data protection is another facet of the digital divide. Today only a few countries have adopted appropriate rules and legislation or set up appropriate institutional arrangements.

This situation raises concerns regarding the fragility of digital learning ecosystems and the lack of capacity to protect learners' data privacy and security (Shiohira and Dale-Jones, 2018). There is a broad agreement that proper rules and protocols are needed to protect students and teachers from overreach. While national policies and regulations are needed, international cooperation and collaborative efforts are also required to support policy learning, knowledge sharing and mutual understanding. The continued reinforcement of learners' data protection and security will require actions to build shared knowledge, norms and standards. While not completely silent on matters of data privacy, ongoing international processes are certainly in need of strengthening.

[1] See https://www.oecd.org/sti/ieconomy/data-driven-innovation.htm

UNESCO has a vital role to play in five key areas:

1 Data protection as a fundamental human right: With the emergence of powerful data mining processes and analytics, technology can aggregate and integrate data to draw far-reaching inferences about individuals' capacities and profiles. Currently, the United Nations (UN) framework does not recognize personal data protection as a fundamental right. By contrast, the right to privacy is a long-established right. UNESCO plans to work with key partners across the public and private sectors to promote this approach, and ultimately, if requested by its Member States, to put in place an internationally agreed normative instrument to recognize personal data protection as a human right.

2 Data for individualized learning experiences and identity: Data can capture the full learning experience of individuals and connect it to other areas of human activity including work, health and leisure. Data analytics can offer personalized, adaptive and flexible learning processes and pathways, an enhanced ability to evaluate the multiple dimensions of learners' competencies, and better-informed education decision-making. In this wider sense, a learner's digital identity is a version, or facet (sometimes also referred to as a 'digital twin'), of a person's social identity that can be used to facilitate mobility, recognition of credentials and transferability of learning records across ecosystems. UNESCO aims to play a greater role in setting the agenda in terms of the methodology and ethical principles to be applied both by public and private institutions managing digital identities and individual learning data (UNESCO, 2022b). To facilitate learners' mobility, cross-border recognition of learning experiences and outcomes and interoperability of ecosystems, UNESCO could possibly create a neutral international repository, or facilitate a global exchange network to enable Member States' recognized authorities to share learning records and preserve privacy and security.

3 Privacy by design: The education sector has traditionally been mindful of the rights of young learners, but less so of the vulnerability of lifelong learners directly associated with their personal data. New privacy laws have gained traction across the globe, and their application and interpretation within education settings requires more attention. Differential privacy is also an important concept to understand. The concept applies to large datasets: an algorithm is said to be differentially private if one cannot tell by looking at the output whether or not any individual's data was included in the original dataset. In other words, the guarantee of a differentially private algorithm is that its behaviour hardly changes when a single individual joins or leaves the dataset. Any output by the algorithm from a database containing a given individual's information is almost as likely to have come from a database without that individual's information.[2] UNESCO aims to play a role in these processes, with a strong emphasis on the development of 'privacy by design' education systems, learning platforms and resources.

4 Privacy as trust: A distinguishing feature of the way students behave in an educational context and share their personal information is their inherent trust in their education providers. The educational context is supposed and considered to be a safe environment. UNESCO argues that education providers and data processors in the educational context should be considered as personal information fiduciaries. By initiating work to outline the legal implications of such a status, UNESCO aims to compel the relevant actors to comply with standards of trustworthiness and encourage national systems to enforce such a normative framework in their legal systems.

5 Data as a driver of better policy in education and training: Leveraging data analytics and AI for better policy is in its infancy in the education sector. While developed economies are investing massively in data industries, including in social sectors such as health and education, low-income countries risk being left behind, creating a widening gap between those who reap the benefits of this new data-driven world and those who do not (UNESCO, 2021). The lack of institutions with the requisite administrative capacity, decision-making autonomy and financial resources limits the real advantages of data in decision-making. In some contexts, the demand for, and the culture of, data-informed decision-making are also lacking.

This publication explores early responses from the education sector to the question of managing data privacy in this era of accelerated digitization, even further accelerated by the COVID-19 pandemic. The publication serves as a clarion call to the sector not only to pay careful attention to data privacy in education, but to take the lead in these developments. Learner data are particularly vulnerable to data breaches in a more digitized world, while those same technologies provide the opportunity for more futuristic notions of 'credentialling' that transcend the formal, non-formal and informal divides that have long impeded our ability to realize the full potential of lifelong learning.

We invite readers to join UNESCO in this important process.

[2] See https://privacytools.seas.harvard.edu/differential-privacy

Introduction

Learners across the world are increasingly vulnerable to privacy and security risks as their life and learning experiences are more digitized, and more online. Considering the educational opportunities afforded by this transformation, accelerated by the COVID-19 pandemic, this report pays special attention to the trade-offs involved in determining how best to protect learners' data. The contribution is timely as the pandemic has catapulted teachers and learners worldwide into online digital environments, where data collection capabilities are typically more extensive, less regulated and less familiar than those used in traditional bricks-and-mortar schools. Though no one can predict how the sector will evolve in the months and years to come, it is safe to assume that the future of education will be characterized by its increased integration of online learning.

In recent decades, operational readiness for online learning has tended to focus on issues of connectivity, infrastructure and the development of online solutions, while data protection, privacy, ownership, governance and security concerns have been treated as afterthoughts. However, the situation brought about by COVID-19 has exacerbated the risks and harms to learners' privacy and revealed the weaknesses in the education sector's approach. As policy-makers and leaders work relentlessly to face and recover from the dramatic impact of the COVID-19 pandemic, there is a collective realization of the accrued vulnerabilities facing our interconnected modern world. This adds impetus to the pro-active consideration of other major societal, economic, environmental, geopolitical and technological risks, in order to evaluate our collective level of preparedness and adjust accordingly. The worldwide pandemic showed how essential online solutions have become to the world's societies and economies, allowing governance, work, education and life to continue, despite a major health crisis and worldwide lockdown. It also highlighted the vulnerabilities inherent in the integration of digital technologies and connectivity into everyday life (WEF, 2020).

Much of life happens online nowadays, be it for work, school, or personal purposes. This includes online shopping, staying in touch, browsing the Internet, and a myriad of other possibilities. The impact of increased connectivity[3] and digital technologies affects individuals, businesses and public authorities alike, transforming economies and societies on an unprecedented scale and at unprecedented speed, and 'blurring the lines between the physical, digital and biological spheres' (Schwab, 2016: para. 2). The digitization of economies and societies is measured by progress and developments in a number of policy areas, including connectivity, people's ICT skills, their use of online services, and the state of development of e-commerce and e-government (Eurostat, 2018). Social media platforms are changing not just the way people communicate, but also business strategies, governance dynamics and how communities live together (OECD, 2019; Eurostat, 2018; WEF, 2016; WEF 2019a).

This new era is powered by an intertwined set of technological advances (including the Internet of Things (IoT), Cloud computing, algorithmic and analytic capabilities and artificial intelligence (AI)), and the world's capacity to produce new data and harness their potential is growing exponentially. The role of data is of paramount significance for the digitization of society, 'the lifeblood of the 21st century economy' (WEF, 2019b), with concurrent dynamics of abundant availability and ever-increasing demand. The insights and inferred information obtained by the 'datafication' of societies and economies are used for a variety of purposes, including for profit (such as advertising and marketing or background investigations), for political motives (influencing and persuading individual citizens), improved public action, public welfare and citizen participation (with the open data movement), and the pursuit of sustainable development (Data Revolution Group, 2014) through initiatives like the UN World Data Forum on Sustainable development,[4] the UN Global Pulse[5] and the Open SDG Data Hub,[6] to name only a few.

People's identities are increasingly digital, including learners of younger and younger ages, as their personal online lives merge with their educational trajectories. The personal data that make up these identities is mostly surrendered unwittingly by young and old alike. While adults might be seen as able to make informed decisions on the matter, even if they struggle to do so, minors cannot, and they are incredibly susceptible to misuse of their personal data. The United Nations Development Group (UNDG) (2017: 10) describes such personal information, also known as personally identifiable information (PII), as:

> 'data, in any form or medium, relating to an identified or identifiable individual who can be identified, directly or indirectly, by means reasonably likely to be used, including where an individual can be identified by linking the data to other information reasonably available' (UNDG, 2017: 10).

[3] The ITU estimates that in 2021, 4.9. billion people were using the internet.
[4] See https://unstats.un.org/unsd/undataforum/index.html
[5] See https://www.unglobalpulse.org/about/
[6] See http://unstats-undesa.opendata.arcgis.com

In this publication we explore the response from the broader education sector to the question of managing data privacy in an era of accelerated digitization. The publication is broadly structured in three parts.

Part 1 of this publication explores the changing context in which students learn today, marked by increased digitization, connectivity and datafication. The publication looks at the responses to digitization from the education sector, including the areas of schooling, higher education, workforce training, early childhood and also non-formal and informal learning. The datafication of education (the collection of data at all levels of education systems including the processes of teaching, learning and school management) is examined, along with the commensurate governance and management responses. The section ends with an appeal for a learner-centred approach to data privacy.

Part 2 looks at how the education sector increasingly exposes learners' data to new and greater vulnerabilities, whether in terms of the privacy, security or integrity of their data, or the potentially unforeseen consequences of the disclosure of this data.

Part 3 reviews the varying approaches to privacy and security and examines existing and emerging responses through protective frameworks, either general or tailored to the educational context, and how they are used to enforce the protection of learners' data. It also considers how non-regulatory responses contribute to a holistic approach to safe learning in the modern world. 'Privacy by design' is identified and promoted as a core principle to protect learners' data and establish rules of engagement, nationally and internationally. The publication ends with suggestions for empowering learners and educators and describes the support structures and resources available at present.

We trust that this work will provide a basis for further research in this area and, importantly, that it will drive up awareness among parents, governments and other custodians of minors that data privacy matters during COVID-19 and will continue to matter in the post-pandemic world ahead.

Part 1: Digitization and lifelong learning

The response to digitization in education

The education sector is no stranger to the digital movement. In 2015, the United Nations General Assembly adopted 17 Sustainable Development Goals (SDGs) to be pursued with the aim of achieving peace and shared prosperity by 2030. Education and training are at the heart of this new global Agenda, with SDG 4 seeking to 'ensure inclusive and equitable quality education and promote lifelong learning opportunities for all' (UNESCO, 2015a: 20). Unleashing the full potential of information and communication technologies (ICTs) is seen, and advocated, as critical to the achievement of this international agenda for education.

The Education 2030 Framework for Action (UNESCO, 2015A) provides guidance for the implementation of the Education 2030 Agenda, and highlights how the focus on lifelong learning and the provision of broad and flexible pathways, in particular, call for ICTs to complement and supplement formal schooling. The Qingdao Declaration (UNESCO, 2015b) addresses a variety of ways in which ICTs and increased connectivity can be leveraged to achieve the Education 2030 Agenda and open up new opportunities for lifelong learning. More recently, the Beijing Consensus on artificial intelligence and education (UNESCO, 2019a) considers the potential ways in which artificial intelligence can profoundly transform education and lifelong learning systems, and aims to frame an appropriate policy response. The Consensus urges stakeholders to explore how AI and data-based analytics can support learning, learning assessments and evidence-based policy planning processes. It emphasizes the need for personalized, adaptive and flexible learning processes and pathways, enhanced ability to evaluate the multiple dimensions of learners' competencies, and better-informed education management systems.

While not completely silent on matters of data privacy, these international processes certainly need strengthening, as the COVID-19 pandemic has accelerated the global transition to digital learning. The Recommendation on the Ethics of Artificial Intelligence that was adopted at the 41st session of the UNESCO General Conference in November 2021 is a step in the right direction.[7] Data privacy is key, as the opportunities brought about by the increased digital transformation of the education sector support the entire continuum of lifelong learning. The lifelong learning paradigm seeks to open up the somewhat rigid walls of education to ensure that all people, at all ages, in all settings and at all levels of education, have opportunities to learn and to continue learning:

> In essence, lifelong learning is rooted in the integration of learning and living, covering learning activities for people of all ages (children, young people, adults and elderly, girls and boys, women and men) in all life-wide contexts (family, school, community, workplace and so on) and through a variety of modalities (formal, non-formal and informal) which together meet a wide range of learning needs and demands (UIL, n.d.: 2).

Schools and classrooms

Because of the flexibility they offer, ICTs, and specifically online solutions, are increasingly being adopted to support teaching, learning, assessments and credentialling, as well as the management of education in a variety of contexts. Education leaders have made significant efforts, for a number of years, to integrate Educational Technology (EdTechs) into their schools and classrooms and to connect their schools to the Internet. The approaches adopted have been both top-down (initiated by governments and ministries of education) and bottom-up, initiated by schools. Blended learning models (combining face-to-face and online learning) are being implemented across the globe, either integrated into classroom practice, or as supplemental, additional practices (Stringer et al., 2019). The COVID-19 crisis and the resulting disruption of education systems has amplified and accelerated these processes. The recent report of the Group of Twenty (G20) provides detailed information on blended education programmes and strategies in those countries, in five areas:

1. Improving access, inclusion and connectivity
2. Creating dedicated education platforms and producing digital teaching and learning materials
3. Using lower-tech media to reach disadvantaged groups

[7] Read the text of the recommendation at: https://unesdoc.unesco.org/ark:/48223/pf0000380455

4 Training teachers and school leaders
5 System-level interventions.

Aside from blended models of learning in schools, the numbers of 'fully online schools', also called 'virtual schools', are growing across the world. The VISCED Project, a two-year European collaborative project partly funded by the Lifelong Learning Programme of the European Commission, led a systematic review of fully virtual schools and colleges at the international level as long ago as 2012 (Pepler and Andries, 2012). It found that there were virtual schools on every continent, though predominantly in the United States (US) and Canada, and that they were prevalent in Australia and New Zealand as well. A report by the market firm HTF Market Intelligence (2019) estimated the US virtual schools' market share to be 93.2% in 2017, with Canada at 3.8% and the EU 0.83%. In China and Japan, virtual schools were reported to have gained in popularity in recent years. The report also predicted more growth for virtual schools by 2024 – and these estimates predated the COVID-19 pandemic, which undoubtedly will affect this growth even more. In the US, despite evidence pointing towards poor performance, over 500 full-time virtual schools were reported as serving about 300,000 students during the academic year 2017-2018 (Molnar et al., 2019).

Higher education

The most significant impact of digitization and connectivity on higher education in the past years has without doubt been the emergence of Massive Online Open Courses (MOOCs), at the intersection of open education and online education. MOOCs have been regarded as one of the most suitable tools to widen access to higher education because of their low cost and flexible entry points. Class Central, a leading search engine for online course offerings, releases an annual industry analysis, reviewing MOOCs statistics and trends. By the end of 2019, eight years since the launch of MOOCs, over 110 million learners worldwide had enrolled in MOOCs, and 900 universities were participating and offering a total of 13,500 courses (Shah, 2019a).

Several universities have also expanded their learning offerings with online and blended learning. With benefits in terms of accessibility and affordability, these online pathways allow for a diversification of learners' profiles, compared to onsite students. Online programmes are a useful resource for working adults seeking to support their career advancement and students facing financial constraints. Georgia Tech's Master's in computer science, for example, launched in 2014, enrolls about 10,000 students who each pay USD 7,000, a sixth of what they would have paid for the in-person programme (The New York Times, 2020).

Workforce training

Online learning, including MOOCs, has been leveraged to serve the workforce for training and continuous development purposes. Businesses of all sizes, government agencies, organizations (from UN agencies to local NGOs) are turning towards blended learning or fully online solutions to support workforce training, onboarding, knowledge retention, etc.

Box 1: Training programmes - IBM Corporation example

The **IBM Corporation**, an American technology company which operates in 175 countries and counted over 350,000 employees in 2019 (IBM, 2019), is repeatedly featured among top training organizations, spending half a billion dollars in employee education every year (Forbes, 2018). The training programmes, in place since 1911, were initially product-focused and relied on in-person courses. But with the advent of accelerated release cycles for new technologies, and with the skills needed changing faster as a result, the company's training turned towards role-based training and took advantage of digitization by offering the bulk of their training online, with over 2,500 courses offered online to date.

For more information: visit *https://www.ibm.com/services/learning/search?trainingType=Course*

Non-formal and informal learning

Non-formal and informal learning have also been impacted. The Education 2030 Framework for Action highlighted the critical role ICTs can play in supporting the development of non-formal learning and informal learning opportunities (UNESCO, 2018c). Google Play Store and Apple App Store, the two leading global marketplaces for apps, respectively feature over 250,000[8] and

[8] See https://www.appbrain.com/stats/android-market-app-categories

75,000[9] education apps. Extracurricular mobile apps are used by millions of learners for a variety of purposes: from tutoring and test preparation to gamification of learning, and the learning of new languages. The free language learning application Duolingo, for example, which uses games to support the learning of about a dozen languages, reports 300 million learners using the software.

Early childhood education

Though less at the forefront of the international conversation around ICTs in education, connected digital media also find their way into early childhood care and education settings (for pedagogical as well as management purposes). An analytical survey in 2010 by the UNESCO Institute for Information Technologies in Education (IITE), 'Recognizing the potential of ICT in early childhood education' (2010), already reported that some early childhood formal education centres were using their websites for children's play and learning. One centre in Campo Maior, Portugal, had, for example, developed a website that gave 'children the possibility to explore other sites on the Internet for play and education, acquiring at the same time more autonomy in their choices or searches'. Common Sense, an American non-profit organization that reviews EdTechs (using criteria of privacy, security and pedagogy), offers a selection of well-rated early childhood education resources on its webpage. In June 2020, 58 early learning apps, games and websites were listed for the attention of preschool and kindergarten teachers.[10]

The datafication of education

Education activities have generated data for many centuries. However, the surge in the use of Internet technologies to mediate teaching and learning results in digital educational data that differ from those in pre-digital contexts. They are more exhaustive in scope, nature and granularity, thanks to new ways of capturing and storing information. The level of combination and aggregation is unprecedented, empowered by ever stronger algorithmic capabilities. As Jarke and Breiter (2019: 1) note in an editorial on the datafication of education: 'The datafication of education comprises of the collection of data on all levels of educational systems (individual, classroom, school, region, state, international), potentially about all processes of teaching, learning and school management.'

The OECD (2020) suggests three categories for the data shared online by children, which can be broadened to all learners:

1. Data given: the data learners provide about themselves (e.g. name or date of birth) (or provided by their parents or educational institution).
2. Data traces: the data they leave online (e.g. through cookies, web beacons or device/browser fingerprinting, location data and other metadata).
3. Inferred data: the data derived from analysing data given and data traces.

The nature of the information can be administrative, 'demographic, behavioural, and educational achievement data for the purpose of administrating or monitoring educational programs and practices' (Ho, 2017: 2), such as name, gender, attendance information or examination scores. The emergence of data reflecting students' progress in learning processes is the most significant change enabled by digitization and online learning solutions, as this information used to be intangible and undocumented (Ho, 2017). Information about a learner's thinking patterns, learning trajectory, engagement score, response times, pages read or videos viewed is now seamlessly captured.

Box 2: Country example: Shuren Jingrui Primary School, China

Shuren Jingrui Primary School in Chongqing, China, is among the UNESCO-Fazheng (UNESCO, 2019e) project case studies on best practices in mobile learning. The entire school is equipped with smart-touch screens and personal tablets for the students, so that their digital traces can be tracked and leveraged for learning purposes. A flipped-classroom pedagogy is implemented: students access the learning resources online before class and get acquainted with the lesson. The platform provides data for teachers on, for example, how many times a student watched an educational video before class, how long they stopped at a certain key point, how many correct answers they gave on a quiz, and what types of errors they made. Based on the analysis of these pre-class learning outcomes, the teacher can prepare the class's interactive and cooperative activities.

[9] See https://www.apple.com/ca/education/ipad/apps-books-and-more/

[10] See https://www.commonsense.org/education/top-picks/excellent-early-childhood-education-resources

As new technologies continue to surface, the nature of the information collected about students even exceeds administrative and learning process categories. Biometric information can sometimes be collected and processed, depending on the country and the legal framework in force. For example, fingerprints or eye scans can be used for verification purposes, to access and complete an examination. Data stemming from the IoT are harnessed to better grasp learners' holistic experience. The AltSchool network of private schools in the US, for example, uses 'cameras, microphones, and electronic devices worn and used by students in order to track every word, fidget, facial expression, heartbeat, click, action, and social interaction for potential research' and to inform decision-making (UNESCO, 2018b: 36).

The datafication of the education sector, combined with developments in AI and algorithmic capabilities, opens up new horizons for personalized and adaptive learning experiences and better learning outcomes, as well as informed governance of education and decision-making. With the emergence of powerful educational data mining processes and learning analytics, technology can aggregate and integrate data to draw far-reaching inferences about learners' capacities and limitations and teachers' performances.

Informed governance and management of education

The proliferation of educational data and the development of AI techniques in education has a profound impact on decision-making (data-driven education decision-making). Educational stakeholders such as schools and institutions, public authorities and policy-makers resort increasingly to these presumedly 'objective' inputs offered by the 'evidence base', in order to govern and manage the education system. Applications range from allocation of resources and staff, teaching evaluation, school inspections and accountability responses to comparative assessments of student achievement at international, national and local levels (Jarke & Breiter, 2019; Aldowah et al., 2019).

These systems are widely used by educational stakeholders at the regional, local and institutional levels, as well as for generating national statistics. Education Management Information Systems (EMIS) have traditionally been said to focus on administrative quantitative data, related to access and participation, such as enrolment rates, attendance, schools and numbers of teachers. This is changing in the context of SDG 4 to reflect a greater focus on learning outcomes, quality, relevance and lifelong learning, and a demand for EMIS to re-orient towards educational outputs and outcomes (UNESCO, 2018b). Intersectoral analysis is another area of growing expectation for EMIS, which should be able to cross educational outcomes with those of other sectors for the advancement of socio-economic development objectives:

> Effective EMIS can help policy-makers in this regard by interfacing with other sectors' information systems and subsequently providing policy-makers with intersectoral data and analyses. These intersectoral analyses can then inform policy and programme development at the sub-national, national, regional, and international levels (UNESCO, 2018b: 20).

Integrated data systems – in which learners' educational records are linked with data from other government departments – are already in place in a number of countries, both at national and local levels. Such integration yields new insights about education, such as a 'holistic understanding of a particular learner's experiences' or 'correlations and causations previously unknown', between education and other development priorities. UNESCO documents the case of a public school district in Pittsburgh, United States, that started to share information from its EMIS about individual students with the municipal department of human services' data centre. Linkages were, for example, established between 'family disruptions such as divorce or domestic disputes and school attendance and performance', helping the 'school staff to look for underlying problems when they saw an increase in absenteeism or a sudden dip in test scores' (UNESCO, 2018b: 35).

Future prospects for 'AI-enhanced EMIS' include access to comprehensive and clear dashboards in support of informed decision-making, and predictive decision-making algorithms (UNESCO, 2019f). In the United Arab Emirates (UAE), an 'advanced data analytics platform' has been rolled out by the Ministry of Education. The scope of the system is significant, with over 1,200 schools and more than 70 higher education institutions participating, covering the data of over 1.2 million students. Information includes 'data on curricula, teachers' professional development, learning resources, financing, operations, performance reports, teacher, student and parent feedback, and scores from international assessments like PISA and TIMSS'. The dedicated data analytics section of the Ministry of Education develops 'machine learning algorithms in support of strategic studies on the country's education system' (UNESCO, 2019f).

Personalized learning for better learning outcomes

AI techniques are used in a myriad of different ways, including for personalized learning plans and trajectories for students, signalling to teachers which students need specific support in a given activity or course, automation of grading and assessment activities, detection of abnormal correlations between students' final marks and online behaviours, enhancement of learning material, and monitoring of collaborative learning settings and social interactions to recommend appropriate learning partners (Aldowah et al., 2019; UNESCO, 2019f). Initiatives to integrate AI-powered EdTechs in education range from State-based to philanthropic and private. A working paper by UNESCO on AI in Education (2019f) illustrates such emerging practices by reviewing worldwide examples, highlighting that many of the 'first-generation AI initiatives in education in developing countries' come from the private sector with a view to profit, or in partnership with public authorities.

Box 3: Country example: Plan Ceibal, Uruguay

Plan Ceibal in Uruguay is the State agency in charge of the digital transformation of education. Leading the adoption of personalized learning at national level, it has adapted the content of an online adaptive learning solution developed by a German company, the 'Mathematics Adaptive Platform', to the national curriculum. The tool 'provides personalized feedback according to each student's skill level based on an analysis of student experiences'. Plan Ceibal's website lists a number of advantages to the adoption of the solution, including 'immediacy of the response; student independence; ease of correction; learning personalisation; classroom gamification; promoting group work; adaptation to the rhythms of class and each student, and a large number of activities'. (UNESCO, 2019f, p.14)

Workforce training solutions are no strangers to the opportunities offered by AI for personalized learning paths. IBM's education system has been described as offering employees a 'Netflix-type experience' (Forbes, 2018). The company developed a personalized learning system, 'Your Learning', introduced in 2016, powered by IBM® Watson™ cognitive technology. Curating the learning it offers to each employee based on their preferences, job history and career goals, the website counts 30,000 learner transactions a day.[11]

Accelerated datafication during the COVID-19 pandemic

With the school closures caused by the COVID-19 pandemic, many countries introduced online learning or accelerated their shift to it. By October 2020, 90% of the 135 countries that responded to the joint survey by UNESCO, UNICEF and the World Bank were using online platforms for remote learning,[12] indicating a significant influx of learners' data collected over a short period of time. Also, the rapidly evolving situation required more timely, granular data for decision-making. To fill the data gaps, some countries enhanced their EMIS while expanding their online learning platforms.

Box 4: Country examples: EMIS tools in Argentina and China

COVID-19 exacerbated gentina's EMIS challenges, including lack of nominal data, connectivity, and timely information. To address these challenges, new EMIS tools were developed, including: SINIDE Acompañar (SINIDE Companion) to monitor attendance and performance of students in secondary education, a teacher vaccination registry, and Cuidar Escuelas, a nominal registry for suspected cases of COVID-19 among students, teachers and staff in order to plan for school reopening.

In response to COVID-19-induced school closures, China launched an initiative called 'Disrupted classes, undisrupted learning', which consisted of developing an online learning platform and providing massive online classes and educational resources. The EMIS allowed the collection and real-time analysis of data from the online learning platform and beyond, with a specific focus on monitoring early warning signs of education risks and monitoring students' attendance.

Source: UNESCO, 2021b, p.5

[11] See https://www.ibm.com/topics/training-development

[12] UNESCO, UNICEF and the World Bank (2020). Survey on National Education Responses to COVID-19 School Closures, round 2. Paris, New York, Washington D.C.: UNESCO, UNICEF, World Bank.

Part 2: How the privacy and security of learners' data is challenged and put at risk

A disproportionate and paradoxical reliance on notice-and-consent regimes for the processing of learners' data

The main feature of the protection of learners' data is the dependence on consent to data processing. However, the heavy reliance on notice-and-choice regimes is flawed for various reasons. To start with, meaningful consent is probably one of the greatest challenges in the current digitized context. Consent can be gathered by opt-out techniques (in which case learners are deemed to willingly consent to the collection of their data unless they explicitly state the contrary), though is it unlikely that this equates to an informed and intentional choice. Furthermore, consent to privacy and security practices (whether opt-in or opt-out) might be more reflective of the need to access the educational service than true acceptance of the terms. This is especially true when the service is chosen by the educational authority, leaving little choice to the learner. When an entire class is using Chrome tablets for example, it may be very stigmatizing, if not impossible, for one child only not to use the device.

The complexity of privacy policies is another challenge to informed consent. Privacy policies are long to read, hard to find and hard to understand. They often contain broad language or an overwhelming amount of complex and detailed information and language. They are rarely read and if they are, rarely understood. A 2018 study led in the US by Common Sense Education (Kelly, Graham & Fitzgerald, 2018), in partnership with 150 school districts across the US, evaluated the privacy policies of 100 popular EdTech applications and services, free as well as fee-based, used by students either at home or in the classroom. Though the study is limited in scope (geography, educational levels and learning settings), its findings illustrate the unlikelihood that users are consenting with full awareness to some EdTech privacy features. It is more likely that these practices, buried in indigestible text, go unnoticed.

Box 5: Examples of findings of a study led in the US by Common Sense Education on privacy policies of EdTech applications and services used by students

Third-party marketing: Thirty-eight per cent of educational technologies evaluated indicate they may use children's personal and nonpersonal information for third-party marketing.

Advertising: Forty per cent indicate that they may display contextual advertisements based on webpage content, and twenty-nine per cent indicate that they may display behavioural advertisements based on information collected from use of the service.

Tracking: Among web-based services, thirty-seven per cent indicate that collected information can be used by tracking technologies and third-party advertisers, twenty-one per cent that collected data may be used to track visitors after they leave the site, and thirty per cent state that they ignore 'do not track' requests or other mechanisms to opt out.

Profiling: Ten per cent indicate that they may create and target (advertising) profiles of their users.

Data transfer: Seventy-four per cent indicate that they retain the right to transfer any personal information collected to a third party if the company is acquired, merges, or files for bankruptcy.

Source: Kelly, G., Graham, J. and Fitzgerald, B., 2018, pp. 9-10. Available under CC BY 4.0

Algorithmic and predictive analysis, combined with big data, 'are built to create their own personally identifiable information, the collection and use of which cannot, by definition, be disclosed in a privacy policy' (Waldman, 2018: 84). To complicate this further, the difficulties of 'unsharing' or revoking data become even more intractable when machine and deep learning models have been applied in educational contexts (Bourtoule et al, 2020). Consent regimes thus protect learners inadequately against the use of the aggregated and integrated sets of their personal data and the information inferred from them. A case in point is the many current EdTech platforms failing to obtain parental consent in case of minors, as mandated by the Children's Online Privacy Protection Rule (COPPA) in the US. For consent to be meaningful, the following evaluation questions should be addressed: Do learners know what personal data of theirs is collected? And why? Do learners understand how data collected about them is used/shared/processed/sold? Do learners understand what they agree to? Do learners understand the value of the aggregated data they disclose? Do learners have a meaningful choice regarding the collection and use of their data?

Scholars have observed and researched a phenomenon they call the 'privacy paradox': a 'discrepancy between the expressed concern and the actual behaviour of users (…): users claim to be very concerned about their privacy but do very little to protect their personal data' (Barth & de Jong, 2017: 1038). A systematic review of the literature on the subject found that:

> a user's decision-making process as it pertains to the willingness to divulge privacy information is generally driven by two considerations: (1) risk-benefit evaluation and (2) risk assessment deemed to be none or negligible (Barth & de Jong, 2017: 1038).

Research in the educational context confirms the existence of the privacy paradox in learners' agency. Though wanting higher levels of control over the processing of their data, the students' stated preferences conflict with their 'low levels of risk prevention behaviours and agency'. Considerations of convenience and the need to receive personalized attention may influence the trade-offs they make (Slade et al., 2019).

Context matters in determining learners' behaviours, and research shows that 'trust in the service provider' is crucial in the way students perceive and manage the privacy of their information. Their desire 'to maintain control (…) lessens when there is a relationship of trust and care' with their educational institution (Slade et al., 2019). Building learners' data protection on the foundation of learners' agency (regimes of notice-and-choice and subsequent control), to use the argument set forth by Waldman (2018), fails to account for the power asymmetries between learners and data collectors and processors caused by the unmanageable disclosure that occurs in online experiences. To ensure that data collectors and processors use the power they have over learners with their best interests in mind, the concept of 'information fiduciaries', who are 'obligated to act in a trustworthy manner' (Waldman, 2018) is particularly relevant.

A commercial ecosystem fuelled by learners' data

Learners' data are valuable to a variety of entities, whether learners themselves and their educators, or policy-makers, advertising juggernauts, data brokers, social scientists, corporations, political parties and employers. Additional 'technical' actors in this data ecosystem include data analytic providers, hardware providers, educational software providers, IT infrastructure providers and Internet service providers. The question of who owns digital learning data arises amid this complex landscape of stakeholders, all the more so in light of the growing involvement of private actors.

Learners are regularly subjected to market forces, such as targeted advertisements or profiling. Students targeted as potential consumers can be faced with various levels of advertising and marketing, from contextual (displaying 'products and services to users based only on the relevant content or webpage the user is currently viewing') (Kelly, Graham & Fitzgerald, 2018: 46), to targeted or behavioural (where tracking technologies provide general and specific information in order to 'display products and services that may be more directed to users, to a more specific targeted audience, than simply contextual advertisements') (Kelly, Graham & Fitzgerald, 2018: 46). A central question facing the education sector is whether learners' data should be collected, used, shared, sold, bought and/or processed for commercial purposes. It could be argued that learners have a reasonable expectation that as they trust educational actors with their data, it will not be used for commercial purposes unrelated to their learning. If their data is used for commercial purposes, learners should know by whom and under what conditions: 'the commercial marketplace for student information should not be a subterranean market' (Russell et al., 2018). Several entities have adopted strong positions on this topic, including the Consultative Committee of Convention 108, which stated that 'educational institutions need strong legislative frameworks and codes of practice to empower staff, and to give clarity to companies to know what is permitted and what is not when processing children's data in the context of educational activities, creating a fair environment for everyone' (Council of Europe, 2021). The Global Privacy Assembly has also expressed the view that 'States should consider promoting regulations prohibiting the use or transmission to third parties of children's data for commercial or advertising purposes and the practice of marketing techniques that may encourage children to provide personal data' (GPA, 2021a).

Questioning the legitimacy of a 'for-profit' approach to learners' data is part of a broader debate around the business models of EdTech providers, and it needs to consider the trade-offs involved. Some have adopted a 'pay to use' or 'subscription' model, others are using a 'data collection and advertising' model, yet others have their cake and eat it too, making profit out of combining the two models. This tension will play into privacy considerations. Some EdTechs offer 'free' services, but no service is ever really free. The idea then is that there is a tacit agreement of sorts: users agree to be 'the product' in order to have free access. But what exactly does it entail? Does it consist of being exposed to advertisements? Of what kind? Contextual, targeted, behaviouristic? Does it mean using one's personal data to 'pay' for the service (and surrendering ownership and control over it)? And are the learners indeed aware that they have entered into such a tacit agreement? Are they fully aware that they are treated as consumers exposed to advertising the moment they use the EdTech? Research points towards a lack of knowledge, understanding and awareness of privacy among youth and children, and in particular 'commercial privacy', relating to 'the incomprehensibility of how their online data is being collected and used (…), how it flows and transforms – being stored, shared and profiled (…), and to what effect and future consequence (…)'. Children also 'display some confusion of what personal data means and a general inability to see why their data might be valuable to anyone' (Livingstone et al., 2019). Even parents, teachers, schools and employers might not grasp the full extent of the agreement they may make on behalf of the learners. While children must be informed about the collection and processing of their personal data, 'there is at the same time a consensus that children cannot be expected to understand a very complex online environment and to take on its responsibilities alone' (Council of Europe, 2021: 7).

A case in point is the Edmodo education platform's recent shift to an advertising business model. In February 2017, the CEO of the platform, which claims over 85 million members and is used by teachers, students and parents, announced through a post on the platform[13] that it would start displaying 'sponsored' or 'promoted content' (ads), in an effort to support its operating expenses while keeping the service free and accessible to its users. The educational platform was careful to specify that there would be no use of personally identifiable information to offer sponsored content according to behavioural profiles (Edmodo, n.d.). The advertising was to be purely contextual. However, shortly thereafter, education privacy researcher Bill Fitzgerald published a blog post which exposed how Edmodo tracked its users' activity and sent the information to data brokers. The researcher mentioned the possibility that the tracking was due to a technical error and/or that Edmodo was potentially unaware of it (which reveals how vulnerable such systems are). His questions echo the point about the fragility of such 'tacit agreements':

> How aware are teachers in the Edmodo community that they are being tracked by ad brokers permitted on the site by Edmodo? How aware are students, teachers, and parents that ad brokers can collect data on students while using Edmodo? How does the presence of ad trackers that push information about student use to data brokers improve student learning? (Fitzgerald, 2017)

In this particular instance, Edmodo reacted quickly, as in early March 2017 they announced that the tracking had been removed from their web application.

EdTech and other big technology companies have a steadily growing influence on education decision-making. Yet at the same time they are profiting from the digitization of educational platforms, built upon the business logic of datafication of education. There have been numerous calls to ensure that private actors respect the ideals of education as a 'common good' (UNESCO, 2015c). The implications also carry over into the privacy and data protection debate.

Long-term and potentially unforeseen consequences of the disclosure of learners' data

'Pedagogical functions', 'decision-making' and 'educational evaluation and credentialling' are increasingly outsourced to data analytics and algorithms, due, in part, to their assumed neutrality and objectivity. These are also called high-risk AI systems.

> In performing these seemingly mundane processes, technologies—and their corporate providers—in fact exercise significant authority over fundamental aspects of education that have previously been invested in teachers, school administrators, and […] policy-makers (Zeide, 2017: 168).

In education and training, these are systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions, and AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for

[13] See https://www.edmodo.com/post/630905359/behalf-Edmodo-Team-I-want-to-be-first-person-to-tell-about

admission to educational institutions. In employment, workforce management and access to self-employment, these are AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications and evaluating candidates in the course of interviews or tests, as well as AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and monitoring and evaluating the performance and behaviour of persons in such relationships.

Greater levels of fine-grained information and permanency of records can expose much more to the public eye than learners initially intended, with potentially significant and long-term consequences. With easy and permanent access to learners' records, every past mistake has the potential to 'flaw' the perception of their learning process. Data-informed decision-making can potentially limit learners' future prospects and opportunities (such as learning trajectories and professional outcomes). Even recorded achievements can become detrimental when used, for example, for the purposes of comparison. The power and potential of analytics mean that educational data is increasingly sought by third parties, including potential future or current employers. When the analysis made of the educational data is to the learner's disadvantage, they face risks such as loss of employability or a negative impact on current employment. Scholars have highlighted that:

> employers already demand transcripts, letters of recommendation, and standardized test scores, and it is easy to see why they would value information tracking students' behaviours and work habits over time (Rubel & Jones, 2014: 13).

Claims that 'students could simply abstain from sharing their data records with employers' are largely ineffectual. Theoretically, people could still abstain from sharing their transcripts with employers, but this will limit the person's employability prospects. In the case of online learning in the context of the world of work, employers are increasingly hosting their own 'learning'/'training' platforms. In this way, they are able to control and see all the backend data, and are thereby equipped to rank and sort employees or even potential employees. A situation in which all major employers would require the completion of a MOOC-like online course for candidates applying for a job is not too far-fetched.

These shifts in decision-making also have 'unintended consequences', due to 'inaccurate or unrepresentative data, algorithmic bias or disparate impact, scientism replacing more holistic and contextualized personal evaluation, and the exclusion of non-computable variables and non-quantifiable learning outcomes' (Zeide, 2017: 169). Scholars and the international community have become more and more vocal about the danger of blindly trusting the supposed 'neutrality' of algorithms: values and opinions are embedded in algorithms, so that 'decisions made by computer are not fundamentally more logical and unbiased than decisions made by people' (Donovan et al., 2018).

The Beijing Consensus on artificial intelligence and education recommends that stakeholders:

> be cognizant that AI applications can impose different kinds of bias that are inherent in the data the technology is trained on and uses as input, as well as in the way that the processes and algorithms are constructed and used (UNESCO, 2019a).

Personal data are ordered through classifications, such as race, gender, ethnicity and socioeconomic status. These categories are an easy vector for the perpetuation of old prejudices. Learners face the risk of being tracked into 'trajectories that limit their potential or are discriminatory' (Plunkett & Gasser, 2016; Villani, 2018).

The occurrence of technological redlining (inequitable outcomes and replication of known inequalities because of biased algorithms) 'occurs because we have no control over how data is used to profile us' (Donovan et al., 2018). Donovan, Caplan, Matthews & Hanson (2018) use the concept of 'black boxed' algorithmic decision-making – first introduced by Frank Pasquale (law professor at the University of Maryland) – to show how 'there is very little understanding' (and therefore very little regulation and oversight) 'over the data processing going on with algorithms'. The concept of 'algorithmic accountability', referring to the 'assignment of responsibility for how an algorithm is created and its impact on society' is thus of growing importance (Donovan et al., 2018).

Difficulty of ascribing accountability for data protection given the intangibility of learners' data

The notion of data location (also referred to as data residency) is volatile as data can be stored in several places at the same time. An additional challenge is the intangibility of data, especially when stored on the Cloud. Personal data can be located anywhere and possibly in multiple jurisdictions at the same time, with no necessary physical proximity to the data subject. Accountability for the processing of learners' data is then harder to ascribe. Even when location and movements of data can be tracked, States have very different approaches to data privacy, security and cross-border flows, and in the absence of mandatory international standards, there are challenges with determining jurisdiction and applicable laws, leading to very low levels of cross-border cybercrime prosecutions. Jørgensen (2018) notes how more and more of the actors involved in the provision of education are online platforms, characterized by their 'transnational nature', and how that also makes it more and more 'difficult for States to address their impact on […] privacy domestically'.

Greater vulnerabilities in the privacy, security and integrity of learners' data

The use of social media and general-purpose video conferencing for student and teacher interactions blurs the lines between the academic and personal spheres. Images of the interiors of students' homes are often visible in video classes and can reveal previously private dimensions of socio-economic backgrounds. Social media profiles may reveal personal information (such as hobbies, sexual orientation, religious or political beliefs) that a student is not comfortable sharing in an educational setting. Students' perceptions of how an educator factors information shared on their social media profiles into their evaluations or education record may limit how freely students engage with their online classroom. Furthermore, there is also an exclusion factor for students who either cannot or do not want to have a social media account or appear on a video call (Reddy & Vance, 2020).

The security of data can be compromised and expose learners to a variety of risks, ranging from identity theft to bullying and blackmail. Very few digital systems – at least thus far – have proved to be fail-proof. Educational records can be particularly sensitive. They can include learners' grades, but also information such as their medical conditions, home situations, disciplinary measures, or even immigration status. The datafication of education is also generative of a much more fine-grained perception of a learner's profile than was previously possible. When these data are stored online, it becomes easier to access them (including unlawfully and maliciously) than when the data were filed in a single location, in an analogue format, or even a digital format not connected to the Internet. Once online, these sets of data can potentially be within reach of any person with access to a computer, the Internet, and some level of pirating skills. The risks concern both public and private educational records. For example, if the security measures in place to control access, encrypt data, etc. are insufficient, data may be disclosed in an unauthorized manner due to the use of insecure connection mechanisms, incorrect platform configuration or human error. A single security breach can expose the data of millions of people.

Box 6: Example of privacy breaches

A serious privacy breach at the **Ministry of Education of British Columbia** (B.C.) (Canada) involved the 'personal information of 3.4 million BC and Yukon students and teachers', which were exposed when a mobile hard drive containing non-encrypted information was lost (OIPC, 2016). As the investigation report of the information and privacy commissioner for B.C. found, 'the Ministry failed to provide adequate security to prevent unauthorized access, use or disclosure' (OIPC, 2016).

The **Ministry of Higher Education of Quebec** (Canada) also experienced a large-scale security breach that was confirmed in February 2020. The personal information of over 50,000 teachers was stolen, and 400 of them have already filed complaints for identity theft (OneTrust Data Guidance, 2020a).

Data can be inadvertently exposed online. Indiana University took down an online tool that exposed over 100,000 students' grades. Serving to calculate grade point averages, the tool was intended for faculty and staff use but somehow became available to students logging into the student system. Any student could view others' grades without their prior consent (Wood, 2020). Hacking incidents can happen on video-conferencing platforms in the middle of lectures, a phenomenon particularly highlighted during the COVID-19 global lockdown. Numerous classes across the world held on the 'Zoom' platform were repeatedly interrupted by hackers – who were often displaying obscene content or threatening students and teachers. As a result, the platform's use for educational purposes was banned in several cities.

Data security can also refer to the 'integrity' of the data in monitoring and credentialling processes, in that it must not be possible to alter or forge that data. Keevy and Chakroun (UNESCO, 2018a: 16) note how learners' data need to be secured in terms of 'identity of the learner, veracity of test responses, bona fides of the granter of a certificate, etc.' and how 'the source of the data […] is one of the potential weak points within the digital credential ecosystem' (UNESCO, 2018a). This has a direct impact on trust in digital credentialling.

To address this concern, various responses are being explored, including technologies such as software programmes that can be integrated and used within Learning Management System (LMS). 'Turnitin', for example, is a service that detects plagiarism. However, some of the verification technologies come with their own privacy issues. In order to ensure monitoring and surveillance of students during online assessments, certain schools have used software to access students' webcams and microphones, which some have argued violated their privacy rights (Foreseman, 2020). Blockchain used as a technology for the digitization of credentials has been put forward as a tool that secures the integrity of the digital certificate, which cannot be forged (Grech & Camilleri, 2017). However, the compatibility of the technology with data protection frameworks has been questioned, 'due to the inability to meet requirements for rectification, erasure, and restriction of processing of personal data' (Future of Privacy Forum, 2020).

Part 3: Protecting learners' data privacy and security

Conceptualizations of privacy and data protection

The idea of privacy carries strong cultural components, starting with variations in the terminology used. By 2019, 132 laws had been adopted regarding the protection of personal information (Greenleaf, 2019a). Following in the footsteps of the European Union and the Council of Europe, which have been using the umbrella term 'Data Protection' in their regulatory texts in the field,[14] over 90 laws (across and beyond Europe, including most of the African countries, Japan, Singapore, Mexico and Uruguay) refer to 'data protection' or 'personal data protection' in their overarching frameworks. A dozen others (such as Brazil, Chile, New Zealand, the United States and Australia) refer to the concept of privacy. Some laws use concepts such as cybersecurity (e.g. China and Guinea) or informational self-determination (Hungary).

Beyond semantics, national regulatory frameworks differ also in their focus. Concepts of privacy differ from country to country, even among countries that are broadly similar. For some, protecting people's privacy is mainly understood as protecting them against the intrusions of non-governmental entities (e.g. European countries). For others (namely the United States), it is commonly understood as protecting people from the risks of government overreach and avoiding interference (Jørgensen, 2018). Specific aspects of data protection may be emphasized, depending on the national context. European countries' legislative frameworks tend to capture both security and privacy aspects. In China, the emphasis of the Cyber Security Law (2016) seems to be more on the security aspect of the data (Samm et al., 2018).

The best way to protect privacy and personal data is also debated, taking into account the beneficial effects of information sharing, with proponents of regulatory solutions on one side, and those advocating private actors' self-regulation on the other. Countries hold different views:

> The European Union has focused on regulatory solutions, establishing principles that govern use of data across multiple sectors, including the need for individuals' consent for certain data processing activities. By contrast, the United States has taken a more limited, sectorial, and ad hoc regulatory approach, often opting for providing guidelines rather than enforcing principles (Acquisiti et al., 2016: 479).

Rights-based conceptualizations of privacy have been the dominant approach to date for the protection of personal information; they have 'had a more profound impact on privacy law than any other theory' (Waldman, 2018). Among these approaches, some base their definition of privacy on negative rights, or 'privacy from something', while others view privacy 'affirmatively for the full realization of the liberal, autonomous self', or 'privacy for something' (Waldman, 2018). Privacy-from-something sets the right of the individual against the outside world, and is characterized by a dimension of separation, 'freedom from the public eye'. Privacy-for-something retains the assumption of separation but focuses on safeguarding the individual's freedom and autonomy, to which privacy is said to contribute significantly (Waldman, 2018). Autonomy and choice are the cornerstones of this conceptualization: individuals should have control over their own personal information and whether or not they wish to disseminate it. This is where the 'doctrine of informed consent' and the 'notice-and-choice approach', common across legislative frameworks, have their roots (Ibid.).

[14] The European Union has repeatedly used the term in its regulatory framework, in its Data Protection Directive in 1995, and as a fundamental human right in its 2000 Charter of Fundamental Rights, as well as in the General Data Protection Regulation (2016). The Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981.

On such a view, disclosure of personal information is perceived as the result of a rational personal choice, a controllable action. This, however, fails to take account of the reality and dynamics of disclosure in the digital era, and how it should influence data protection norms. A significant portion of individuals' online activities does not involve voluntary or conscious disclosure (such as browser history, terms searches, cursor activity or IP addresses). If the disclosure of information is systematically perceived and treated as a free choice to waive privacy interests, the 'burden of responsibility' is then entirely on the individual – an obvious power imbalance in light of the constant and ongoing disclosure induced by online activities, 'an illusion of empowerment' (Hartzog, 2018).

Social theories of privacy call for a better reflection of the power dynamics at play in a digital context (including the inevitable – and to some degree uncontrollable – disclosure of personal information). These theories consider how disclosure is inherently influenced by reliance on social norms – 'rules that feed into our expectations of what should happen with our personal data' (Waldman, 2018: 6). According to such theories, flows of personal information are governed by 'context-relative informational norms', which vary according to the social context and 'evolve over time, particularly as new technologies change information flow practices'.

Alluding to the similarities in power dynamics with models such as fiduciary-beneficiary arrangements, scholars are calling for legislative frameworks to protect, as private, 'information disclosed in contexts defined by trust':

> The law of information privacy, then, gives effect to that norm by using both its coercive and expressive power to protect trust, repair it when it breaks down, and constrain the power of data holders. Under privacy-as-trust, lawsuits against those that invade our privacy, statutes that protect our information, legal rules that govern relationships between consumers and data collectors, and judicial opinions on vanguard privacy problems would focus on both expressing the value of relationships of trust and protecting them from harm by limiting the uses of our shared information in accordance with our social expectations (Waldman, 2018: 67).

Interestingly, the concept of 'privacy-as-trust' (Waldman, 2018) has been reflected in the terminology of the Indian Personal Data Protection Bill (2019). Data controllers are referred to as 'data fiduciaries' (Greenleaf, 2020). The concept has also started to appear in international conversations around digital transformation. The World Economic Forum is host to a Global System Initiative on Shaping the Future of Digital Economy and Society. Pursuing the delivery of responsible digital transformation, the Forum calls for the protection of trustworthy systems and for culture 'to pivot towards a new business attitude that accepts data as entrusted and borrowed rather than extracted or taken' (WEF, 2019c: 10).

Economists have developed economic theories around privacy and its informational dimension.[15] Their interest in the topic arises from the fact that the trade-offs associated with the level and features of privacy protection involve economic consequences, especially in a digital age and information societies. Individuals have become producers of highly personal data and leave many digital traces, which used to be in the private domain, and carry substantial economic value. The economic benefits yielded by increased availability and processing of personal data can potentially profit both data subjects and data holders. Though it plays a role in redistributing the balance of economic power among parties, control over personal data involves trade-offs that are more nuanced. In their review of 'the theoretical and empirical economic literature investigating individual and societal trade-offs associated with sharing and protecting personal data', Acquisiti et al. (2016: 443) find that there is no unambiguous conclusion as to 'whether privacy protection entails a net "positive" or "negative" change in purely economic terms: its impact is context specific'. They outline five considerations that influence the economic trade-offs:

1. 'Individuals can directly benefit from sharing their data' (for example through personalized services or discounts).

2. 'Both positive and negative externalities arise through the complex interplay of data creation and transmission' – meaning that when individuals share their information, it may benefit society as a whole (or other individuals), or conversely negatively affect other people (on a societal or individual level).

3. 'Privacy trade-offs often mix the tangible (the discount I will receive from the merchant…), with the intangible (the psychological discomfort I experience when something very personal is exposed without my consent), and the nearly incommensurable (the effect on society of surveillance; the loss of autonomy we endure when others know so much about us).'

4. 'Privacy has elements of both a final good (one valued for its own sake), and an intermediate good (one valued for instrumental purposes)', yet approaches to valuating privacy primarily capture it as a final good.

[15] See https://en.unesco.org/inclusivepolicylab/analytics

5 'It is not always obvious how to properly value privacy and personal data.' The way prices are set is usually determined by the market. But in the case of privacy, 'there is yet no open, recognized market for personal data in which data subjects themselves can participate'; the buying, selling and trading of personal data happens among firms. Moreover, individuals' true valuations of privacy can hardly be inferred by their behaviour or the choices they make, including because in most cases, the trade of their personal data is a 'secondary, mostly inconspicuous, and often altogether invisible aspect of a different, more salient transaction (having a question answered, interacting with peers online, and so forth)' (Acquisiti et al., 2016: 447-448).

The question of the value of data opens up a related discussion beyond the protection of the privacy of information: the protection of economic rights over data (for individuals, groups, communities, even countries), recognizing it as an economic resource (Singh, 2019).

Developments in technology further help shape ideas about privacy. Privacy is mentioned in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). However, the relevant articles (12 and 17, respectively) hinge on the definition of 'arbitrary interference', reflecting the concerns of the framers of the 1948 UDHR and 1966 ICCPR, who could scarcely have imagined the privacy implications of today's technology. Recognizing the impact of rapid technological developments on various actors' capacity to potentially violate the human right to privacy in new ways, the UN High Commissioner for Human Rights has submitted three reports since 2014 on the subject of the right to privacy in the digital age, in response to requests from the UN General Assembly and Human Rights Council.[16] The idea that someone could see a satellite image of someone else's home seemed, just 15 or 20 years ago, a serious violation of privacy. Today it is mundane and widely accepted. People did not usually share pictures publicly; now over 100 million photos are uploaded to a single platform, every day.

Understandings about the privacy of information related to learning have changed over the past century. Privacy 'intrusions' related to learning records have shifted gradually from human mediators (employers and academic admissions committees prior to the 1950s sought information directly from teachers) to quantitative and standardized assessments with their greater (assumed) objectivity. While the idea of keeping and sharing a complete and holistic educational dossier – containing every essay, test score, attendance record, teacher evaluation, certificate and online badge logged for a particular learner – may strike us as an affront to privacy in 2021, this could quickly become normalized. However, that is not to say that movements to protect privacy should merely react to technological developments. Governments could ask technology companies to build tools and utilities that can accommodate their views and expectations regarding privacy, instead of letting a handful of companies exercise increasingly monopolistic control over our ability to access education, learning and information. Regulation does not have to conform to existing technological norms.

Protective normative frameworks in place

Privacy as a human right

Privacy is recognized and protected as a human right through a set of international legal texts, the most notable of which are the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).[17]

Box 7: UDHR and ICCPR articles on privacy

Article 12 of the UDHR
No one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the ICCPR
1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

[16] 2014 Report, A/HRC/27/37*; 2018 Report, A/HRC/39/29, 2021 Report A/HRC/48/31.

[17] The right to privacy is embedded in other international Conventions as well, such as the Convention on the Rights of the Child (Article 16); the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (Article 14); and the Convention on the Rights of Persons with Disabilities (Article 22).

In 2015, the Human Rights Council decided to appoint a Special Rapporteur on the right to privacy, responsible among other things for making recommendations to ensure the promotion and protection of the right to privacy in connection with the challenges arising from new technologies.[18] In 2021, the Human Rights Council published a new report of the Special Rapporteur,[19] which focuses on two separate challenges: firstly, artificial intelligence and privacy, then children's privacy, particularly the role of privacy in supporting autonomy and positive participation in society.

Box 8: Privacy, new technologies and gender perspective

In 2019, while focusing on privacy and gender, the Special Rapporteur recalled in his report (Report of the Special Rapporteur on the right to privacy, 2019) that both the General Assembly (Resolution 71/199) and the Human Rights Council (Resolution 34/7) had called upon States 'to further develop or maintain, in this regard, preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular adverse effects on women, as well as children and persons in vulnerable situations or marginalized groups'.

In fact, while the digital space has the potential to improve the promotion and enjoyment of human rights, it can also reproduce and amplify existing disparities and discriminations and give birth to new forms of violence (Special Rapporteur's report on violence against women, June 2018). In this sense, it has been reported that peoples' experience of digital technologies and privacy is affected by several factors related to their background, including gender or sex characteristics (Report of the Special Rapporteur on the right to privacy, 2019). While privacy is always important, it can be seen as even more crucial for those who face inequalities because when this right is violated, the consequences can be greater for people who already faced discrimination in the non-digital world (Ibid.).

With the education sphere integrating more and more digitalized tools and new technologies such as AI, it should pay particular attention to issues that can arise in relation to the right to privacy and the gender dimension, in order to avoid exacerbating pre-existing inequalities. Furthermore, with the COVID-19 crisis, many education institutions had to rely on the private sector, using social media and different kinds of applications, in order to ensure a quick response to the disruption of education. This was done sometimes by waiving the requirements of basic protection principles such as child data privacy laws, and by choosing tools based on financial considerations rather than privacy (Report of the Special Rapporteur on the right to privacy, 2021), thus leaving more room for breaches of privacy, and potentially putting those already facing discrimination at greater risk.

However, as recently emphasized by the Special Rapporteur on the right to privacy 'Educational processes need not and should not undermine the enjoyment of privacy and other rights, wherever or however education occurs, nor intensify existing inequalities.' (Ibid. p.17)

Provisions in regional human rights legal instruments also offer protection for the right to privacy: the Charter of Fundamental Rights of the European Union; the Treaty on the Functioning of the European Union, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the American Convention on Human Rights, the Arab Charter on Human Rights, the African Charter on the Rights and Welfare of the Child, and the ASEAN Human Right Declaration.

Data protection principles have traditionally been 'encapsulated by the right to privacy', but 'data protection is also emerging as a distinct human or fundamental right' (United Nations, 2009). The Charter of Fundamental Rights of the European Union, which entered into force in 2009, distinguishes a separate, specific right to data protection, in addition to the right to privacy. The ASEAN Human Right Declaration protects the rights of every person 'to be free from arbitrary interference with his or her privacy' and adds that this includes personal data. Human rights law imposes both positive and negative obligations on states. The negative obligation prohibits the state from interfering, except where the law allows. The positive obligation requires the state to take measures that prevent third parties from unlawfully interfering with individuals' privacy. The affirmation of a human right to privacy should have as its corollary a system of protective regulatory and legislative frameworks.

[18] See https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx
[19] See https://undocs.org/A/HRC/46/37

General legislative and regulatory frameworks for privacy and data protection

Box 9: Reimagining our futures together – extract

Developments in biotechnology and neuroscience have the potential to unleash the engineering of human beings in ways that were previously inconceivable. Proper ethical governance and deliberation in the public sphere will become increasingly urgent to ensure that technological developments that affect human genetic make-up and neurochemistry support sustainable, just and peaceful futures… Properly steering these emerging developments in neuroscience and biotechnology will depend on open data, open science and an expanded understanding of the right to education to include rights to connectivity, to data, to information and to the protection of privacy.

Source: Reimagining our futures together, UNESCO, 2021, pp. 37-38.

Many of the challenges brought about by technological developments and increased connectivity do not affect learners alone. Therefore, many of the legislative and regulatory frameworks in place for the protection of privacy are not specific to the educational context, but general in scope. They range from privacy laws to digital data protection laws and consumer privacy laws. In most countries, these non-specific frameworks are used as a baseline for the protection of learners' data, and may be complemented by school policies, contractual arrangements between an educational institution and an EdTech provider, Ministry of Education guidelines, etc. Given the particular vulnerability of children online and the dangers to which they can be exposed, a body of legal texts aims to protect their privacy in digital environments and is used for the protection of students of that age group. In a few cases, however, specific laws have been adopted that target the privacy of students in particular, some even specific to the context of online learning. The following overview of the various frameworks that can be harnessed to protect learners' data shows that, while regulations do not need to be specific to learners' online activities, it is however important to ensure that learners' rights are effectively protected in new and dynamic technological environments. It may be argued that some legal frameworks, though not specific to the educational context, are even broader in the protection they offer than sectorial laws. Good regulations and protections should be enforceable across the applicable jurisdictions, while being able to accommodate new and shifting technologies.

A number of international and regional organizations, from the Global Privacy Assembly (GPA) to the European Union, the Council of Europe, the OECD, and more recently the African Union and the Asia Pacific Economic Cooperation (APEC) have adopted privacy and data protection frameworks.[20]

The OECD Guidelines on privacy (1980) and the Council of Europe Convention 108 (1981) were drafted during the same period, and overlap in many ways. Both texts have substantially influenced the standardization of many of the data protection regulatory frameworks in place across the globe. They have been labelled 'the first generation of international data privacy standards' (Greenleaf, 2019b). New normative influences on current legislative developments go further in the levels of protection they provide, but the following basic standards are commonly found across regulatory frameworks (Greenleaf, 2019b):

- Regarding data processing:
    - Lawfulness of processing: the basis on which data was collected and will be processed should be 'lawful' or 'fair'.
    - Limitation and proportionality of collection, whereby collection of personal data should be limited to what is relevant and necessary for the purposes for which they will be used.
    - Specification of purpose and limitation of use: the purposes for which data are collected should be specified, not later than the time of collection, and there should be limits on their subsequent use and disclosure.
    - Data quality: this concerns the accuracy and relevance of the data.
- Data security: the processing of personal data is to be protected by security safeguards.
- Openness and transparency: Information should exist and be made available regarding the processing of data in order to inform the data subject.

[20] The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (1981) and the protocol amending it (108+), the States Parties to which are steadily expanding beyond Europe, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (originally adopted in 1980, revised in 2013), the European Data Protection Directive (1995), the Global Privacy Assembly's (previously International Conference of Data Protection and Privacy Commissioners') International Standards on the Protection of Personal Data and Privacy (2009), the African Union Convention on Cyber Security and Protection of Personal Data (2014), which has not yet come into force, and the APEC Privacy Framework (2015).

- Rights of the data subjects: Individuals are to be given rights regarding their data: ensuring they can access it and make sure it is correct and complete.
- Accountability: the data processor needs to be accountable regarding compliance.

The latest regulation to date, the European General Data Protection Regulation (GDPR) (2016), is considered by scholars as international best practice. Its scope is general, as the name indicates, yet its provisions are applicable to learners, independently of the context of their learning. A detailed case study of how this general framework applies to learners' data is offered at the end of this section.

At the national level, over 71% of countries have enacted data protection/privacy laws.[21] In the wake of the GDPR and the amended Convention 108 of the Council of Europe, many countries have already updated their privacy laws since 2017, while numerous others are engaged in a revision process, and close to 30 are passing new bills (Greenleaf, 2019c).[22] The European instruments have become international reference points for many countries, and 'the impetus to update existing laws, in order to make them potentially GDPR-compliant, has become a significant driver of international law reform (…) the most important data privacy development in 2018' (Greenleaf, 2019c). In 2018, Africa was reported as the region outside of Europe with the 'most rapid current change in data privacy laws', demonstrating 'to a surprising extent the (…) higher standards found in 2016 EU GDPR' (Greenleaf & Cottier, 2018).

Box 10: Example of States' laws on data privacy

The General Data Privacy Law of **Brazil** (Law No. 13,709 of 14 August 2018) was originally supposed to come into force in January 2021, but amidst disruptions caused by COVID-19, it has been postponed to later in the year. The provisions of the law are largely aligned with the EU GDPR, including the establishment of a Data Protection Authority and restrictions on data transfers (Greenleaf, 2019c).

Uruguay was the first country to accede to Convention 108 though not a Member of the Council of Europe,[23] and is already a signatory to its amended version Convention 108+. It is also among the rare countries that the European Union considers as offering adequate levels of protection, and as such an 'adequate jurisdiction' to receive transfers of personal data from the European Union. It undertook a revision of its data protection law to maintain these statuses, strengthening provisions with regard to its scope (now extra-territorial), data breach notifications, accountability and data protection officers (Greenleaf, 2019c).

The **Indian** Data Protection Bill (2019) is currently being discussed and includes 'many influences from the EU's GDPR'. The Bill employs unusual terminology, not yet found in other laws, but reflective of social privacy theories based on trust: data controllers are referred to as 'data fiduciaries' (Greenleaf, 2020).

The vast majority of these data protection laws are complemented by the establishment of data protection authorities. Several examples of their enforcement activities (such as investigations, rulings and fines) illustrate how these bodies apply general frameworks to sector-specific cases, including in educational contexts. Singapore's Data Protection Authority, the Personal Data Protection Commission (PDPC) fined Marshall Cavendish Education Pte. Ltd. 40,000 Singapore dollars in 2019 for violating the Personal Data Protection Act of 2012. Marshall Cavendish had suffered a ransomware attack, affecting the learning management system that it was providing for the Ministry of Education. Personal data had been exposed to unauthorized access (OneTrust Data Guidance, 2019a). In 2019, the Norwegian data protection authority ('Datatilsynet') fined the Education Agency of the City of Oslo the amount of €120,000 for insufficiently securing data processing in the Skolemelding mobile app. The application was used for communication purposes between school employees, parents, and students. The municipality failed to implement technical and organizational measures ensuring an appropriate level of security given the risk, and preventing communication of sensitive data (such as pupils' health data). The findings of Datatilsynet prompted a quick response by the municipality, which was willing to resolve the issues (OneTrust Data Guidance, 2020b).

The example of the Danish Data Protection Agency (DDPA), the first European data protection authority to issue a ruling on cloud computing for a school system, is another case in point. In the Odense Municipality case, the Danish municipality decided to use Google Apps within its school system in order to process 'sensitive personal data when registering information about

[21] See https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[22] For a detailed overview of these data privacy laws and bills, see Greenleaf, 2019a.
[23] See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=y5LyBqwG

lesson planning and assessments of lesson plans and individual students' educational development' (ITU, 2012). The DDPA opposed this decision on security grounds, in light of the confidentiality and sensitivity of the data. The issue was that the municipality could not ensure that its data processor would meet the Danish Data Protection Act's requirements in terms of security measures – given that it did not know where the data were physically located.

The European GDPR: a case study of how a general framework applies to learners' data

The European GDPR, which came into effect in 2018, has global implications, because of its extra-territorial scope and the scale of the fines that data protection authorities can enforce in case of non-compliance (2 to 4% of companies' worldwide turnover). Some have even spoken of a 'legal revolution' precisely because of those two features (Villani, 2018). The GDPR applies to any organization worldwide processing the personal information of EU residents (whereas the previous Data Protection Directive was only applicable if the organization had infrastructure within the EU). For educational institutions, even those without a physical presence established in Europe, are likely to interact with students based in the EU if they run distance education programmes. The same goes for online education platforms. The GDPR distinguishes two main roles held by either individuals or institutions: the data controller (who 'determines the purposes and means of the processing of personal data') and the data processor (who 'processes personal data on behalf of the controller'). Schools or universities will typically be the controller and EdTechs the processors. EdTechs can also be considered data controllers when the educational service is not provided by the intermediary of a school but directly to the learner.

The definition of data protected under the GDPR is broader than in many national regulations worldwide – including for example people's IP addresses. Responding to the calls for a non-industry approach, GDPR stands as a 'one-size-fits-all' type of regulation, regulating almost all personal data transactions. This means that learners' data are covered by the regulation, whether they are in school, at university, at work or learning online. It stands in stark contrast with national systems in which a learner's status with regard to the legal protection of his/her privacy will heavily depend on contextual factors. The GDPR also requires organizations to maintain records of the processing activities under their responsibility, describing among other things the purposes of the processing, how and to whom the data will be disclosed, transfers to third countries, etc. This implies that educational institutions will need to review all the types of personal data they collect and audit how they process them, not only for their students, but for parents or teachers as well. When the processing of personal data implies 'high risk to the rights and freedoms of natural persons', a data protection impact assessment is required prior to the processing.

If an organization is using a third party for storage and processing of students' data, that third party must prove compliance with the GDPR and the processing shall be governed by a contract, for the organization to be legally allowed to continue to use those services. This means that schools, for example, will need to ensure that any EdTech they work with is compliant with the GDPR, and secure a contract with that processor. This, per se, implies that every EdTech used by the school has to be identified. A New York Times article showed how Google often bypasses education officials in order to promote its products directly to teachers (New York Times, 2017). Under the GDPR, schools cannot afford to be unaware of what is being used in the classrooms. Failure exposes them to GDPR breaches.

The GDPR grants individuals increased control over their personal data by strengthening and creating new rights which they can enforce against those controlling and processing their data, including the right to access their data, to have them rectified or erased, to restrict their processing, to have their data in a portable format, and to object to the processing of their data, including automated individual decision-making and profiling. Schools, companies, EdTechs and any other controller or processor of learners' data need to adapt their privacy policies and practices to accommodate requests for these rights to be exercised.

Automated decisions based on algorithms are at the centre of many debates around learners' privacy, and the European regulation provides for precautionary measures in this regard. The GDPR provides that data subjects have a right to be informed of 'the existence of automated decision-making, including profiling, and […] meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'. The European Commission published a report on automated decision-making practices in the United States and mentions a case where the use of algorithmic-influenced decision-making would have been problematic under the GDPR. Under the GDPR, an explanation of the functioning of the algorithm cannot be withheld from the individuals to whose data it is being applied:

> Public school teachers in Houston, Texas, challenged the use of an algorithmic process introduced in 2012 to assess teacher performance. The assessment process involved a statistical model called the Educational Value–Added Assessment System (EVAAS) developed by SAS, a private software company, and licensed for use by the Houston school district (the District). After adopting the EVAAS model, the District implemented a policy whereby it terminated the employment of teachers who did not

> achieve a certain rating under the model. SAS treated the algorithm as a trade secret and did not divulge it either to the District or the teachers (European Commission, 2018a: 91).

The European regulation calls for technical and organizational measures ensuring the security of processing of personal data. Data breaches are often pictured as the work of malicious actions by hackers, but they can be the result of unintentional human mistakes. The example of an online learning system that stores the personal work of students is a relevant example to review in more detail. If one of the teaching staff has been downloading the personal data of the learners onto his/her computer to grade work, for example, but then loses the device, there is a data breach. Hence the need for reinforced measures of protection, such as pseudonymization and encryption. The GDPR promotes the adoption of certification mechanisms to demonstrate compliance with security requirements. The GDPR also includes 'privacy by design' and 'privacy by default' requirements, whereby data protection for processing and information systems should be built in from the start.

Consent is one of the legal bases proposed by Article 6 of the GDPR, which states that the lawfulness of processing is dependent, in most cases, upon the consent of the data subject. Schools, however, in delivering education, are considered to be performing a task in the public interest and thus can lawfully process data in that capacity. However, this means that the data collected for this purpose cannot be re-used for any other purpose than the public one of education, otherwise they would need to seek consent. A parent's email address, for example, cannot be shared with a third party that promotes school events, under the guise of a 'public task' – the consent of the parent would need to be sought. Similarly, 'schools should also seek consent if they set up a student account on a cloud-hosting service' (School Education Gateway, 2018). The regulation gives details about the requirements relating to that consent. It must be informed and specific to the matter, freely given, and as easy to withdraw as to give. The processing may also be based on a contract. In this case, the data may be processed only to the extent that the execution of the contract, including the provision of a service, makes the data processing necessary. Mandatory disclosures to data subjects in cases of data collection include, among other things, the legal basis and purpose of the data collection, the category of recipients of the personal data, data storage and deletion policies, where applicable, intended transfers of the personal data to a third country, and information on the rights the data subject can exercise.

Transfers of personal data outside the European Union were already regulated by Directive 95/46/EC of 24 October 1995. This protection has been included in the GDPR, which includes the principle whereby transfers to a third country are in principle prohibited, unless that country benefits from an 'adequacy decision' of the European Commission. In the course of this process, the protection of personal data is evaluated (every 4 years) with regard to a list of criteria, including: respect for human rights and fundamental freedoms, legislation on personal data, the effective and enforceable rights of individuals, access of public authorities to personal data and the existence of a supervisory authority and its effective action. At the time of writing, 14 countries have been granted an adequacy decision.[24]

With regard to the United States, the Privacy Shield previously in force was invalidated by the Court of Justice of the European Union in July 2020.[25] The European Court considered that the US law on access to data by intelligence services did not provide a level of protection equivalent to that of the EU, and found a lack of effective remedies in the US essentially equivalent to those required by Article 47 of the EU Charter of Fundamental Rights. This decision has a major impact as it reinforces the accountability required by the GDPR, by insisting on the need for data controllers and processors to ensure that the countries to which they transfer data have legislation compatible with that of the European Union, in terms of fundamental rights and effective guarantees of the rights of the persons involved. Following this judgment, the European Data Protection Supervisor issued a decision finding that the European Parliament had infringed several articles and regulations regarding data protection (related to the use of a COVID-19 test booking website), including regarding EU-US data transfers that did not respect the 'Schrems II' ruling.[26]

Ethics in Artificial Intelligence and data

An important component of the work on data is the work on ethical use of Artificial Intelligence (AI). The UNESCO General Conference recently adopted a Recommendation on the Ethics of Artificial Intelligence (November 2021). It includes several guiding principles regarding data protection and security:[27]

[24] As of January 2022: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay, see https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

[25] Judgment of the Court of Justice of 16 July 2020 in case C-311/18, Data Protection Commissioner v. Facebook Ireland LTD and Maximillian Schrems ('Schrems II'), EU:C:2020:559.

[26] See Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament: https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf

[27] Paragraphs 32, 33 and 34 of the Recommendation, available at: https://unesdoc.unesco.org/ark:/48223/pf0000380455

> Privacy, a right essential to the protection of human dignity, human autonomy and human agency, must be respected, protected and promoted throughout the life cycle of AI systems. Adequate data protection frameworks and governance mechanisms should be established in a multi-stakeholder approach at the national or international level, protected by judicial systems, and ensured throughout the life cycle of AI systems. Data protection frameworks and any related mechanisms should take reference from international data protection principles and standards concerning the collection, use and disclosure of personal data and exercise of their rights by data subjects while ensuring a legitimate aim and a valid legal basis for the processing of personal data, including informed consent. Algorithmic systems require adequate privacy impact assessments, which also include societal and ethical considerations of their use and an innovative use of the privacy by design approach. AI actors need to ensure that they are accountable for the design and implementation of AI systems in such a way as to ensure that personal information is protected throughout the life cycle of the AI system.

The European Union has also launched a proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (the Artificial Intelligence Act).[28] The proposal includes specific provisions related to processing of personal data for developing AI systems, notably high-risk AI systems. In 2021, the European Union put in place an expert group for the development of ethical guidelines on artificial intelligence and data in education and training based on the Ethics Guidelines for Trustworthy Artificial Intelligence, presented by the High-Level Expert Group on AI in 2019.[29]

Specific frameworks protecting children and/or learners

Research has shown that though 'privacy is vital for child development', children are more vulnerable than adults when it comes to privacy and data protection online,[30] 'due to their lack of digital skills or awareness of privacy risks (…) particularly in relation to longer-term effects' (Livingstone et al., 2019). Across the world, there is growing recognition that children deserve special protection in terms of their privacy and personal data, and a number of regulatory efforts are emerging. Though not specific to pupils, these normative instruments can affect how children's data are processed in the educational contexts. A specific right to privacy for children is enshrined in the UN Convention on Protection of the Child (Article 16). In 2021, the Committee on the Rights of the Child, which monitors the implementation of the Convention, developed a General Comment on children's rights in relation to the digital environment that includes consideration of, and guidance on, child privacy and data protection. It embeds online rights into the larger framework of the UNCRC and highlights the risks children face as well as the opportunities the online environment brings, exhorting those responsible to take concrete action.[31] The purpose of the General Comment is to strengthen the case for greater action and elaborate what measures are required from States in order to meet their obligations to promote and protect children's rights in and through the digital environment, and to ensure that other actors, including businesses, meet their responsibilities.

The 2012 OECD Recommendation on the Protection of Children Online (OECD, 2012a), as amended in 2021, calls on governments to put in place a more protective legal and political framework for children in the digital space. It calls for better consideration of technological developments by all public and private actors. In addition, the OECD has published Guidelines for Digital Service Providers, which providers are expected to follow when taking actions that may directly or indirectly affect children in the digital environment. The EU GDPR includes specific provisions for protection of children's personal data in relation to the offer of information society services directly to a child. The modalities for expressing consent described in this article do not apply to other situations.

At the national level, some countries have specific legal provisions to protect children's privacy. In the United States, several federal and State laws overlap in protecting learners' data. One federal law specifically seeks to protect children's privacy online: the Children's Online Privacy Protection Rule (COPPA) of 1998. It prohibits the collection, use and dissemination of personal information from children under the age of 13 without parental consent. This law was used as the legal basis for a privacy complaint against Google's G Suite for Education by the Attorney General of New Mexico in February 2020, illustrating how laws that are not specific to the educational context nevertheless can in some cases offer adequate protection of learners' data. The Attorney General accused the company of collecting personal information of children under age 13 without parental consent, in violation of COPPA provisions. The collected data included physical locations, browser history, videos watched on YouTube, voice recordings, passwords and other behavioural information (State of New Mexico vs Google LLC. 2020).

[28] See https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

[29] See https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3774&fromMembers=true&memberType=5&memberId=96163

[30] The EU GDPR also states in its introduction that 'Whereas: … (38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.'

[31] See https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

A few regulatory frameworks are specifically tailored to provide for students' privacy in educational contexts, including emerging laws that target online learning environments. At the international level, the Global Privacy Assembly (GPA) established a digital education working group (DEWG) in 2013.[32] The Group adopted a Resolution on e-learning platforms in 2018 (ICDPPC, 2018), urging both educational authorities (including Ministries of Education, school boards, school administrators and educators) and online-learning platform manufacturers and providers to respect students', parents' and educators' rights to the protection of their personal data and privacy, and to guarantee that the data collected was solely used for educational purposes in compliance with data protection law.

The UNESCO Institute of Technology in Education has also developed a Guidance Handbook to guide students, teachers and parents in protecting their personal data and privacy in online learning. It identifies security risks and suggests specific strategies to protect personal information in three contexts: before, during and after learning.[33] The Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents handbook is based on the Personal Data Security Technical Guide for Online Education Platforms, which was launched by the UNESCO IITE and Tsinghua University in May 2020. Both the Handbook and Technical Guide complement each other to promote data security for teachers.

The Rewired Global Declaration on Connectivity for Education, aims at providing guiding principles and directions to better ensure that technology fulfils the diverse and ambitious objectives for education including SDG4. The Declaration provides an appropriate framework for the educational promises of technology to be realized by adhering to principles that put technology at the service of learners, teachers and educational institutions. The box below contains the provision regarding learners' data protection.

Box 11: Provision of the Rewired Global Declaration on Connectivity for Education related to data protection

The ease of data capture, storage, and surveillance in digital spaces must be a primary concern for education. It should help improve teaching and learning rather than merely document and control it. Used appropriately, data can clarify what interventions are more and less effective and guide their future development. Most data should be anonymized by default, particularly data used beyond the level of schools, so it cannot be traced back to individuals. Proper rules and protocols are needed to protect the rights of learners, particularly children. Education is a site of experimentation and identity formation, and students need freedom to take risks and make mistakes in online and offline environments built on trust and goodwill. An ethic of transparency and 'do no harm' should guide data policies. All stakeholders should be aware of what data is being captured and for what purposes. This disclosure must be easily comprehended and include options to communicate problems and seek recourse. Educational institutions should work to assure individuals own and control their personal data, and, in the case of children, families should be actively involved in decision-making. When possible, learners should be able to 'opt-out' of data capture and still retain full access to educational opportunities.

Source: Rewired Global Declaration on Connectivity for Education UNESCO, 2022, p.10

At the national level, the United States' legislative apparatus offers examples of one text protecting students' education records, and others regulating EdTech companies in order to protect students' online personal information. The Family Educational Rights and Privacy Act (FERPA) is a 1974 federal law designed to apply to schools and educational institutions and to protect the privacy of student education records from unauthorized disclosures. Its adoption at a time when online educational services were not yet on the radar raises the question of whether the instrument can adequately address the impact of the digital age on privacy of student records. Not all student information used in online educational services is protected by FERPA, and it is up to schools and districts to evaluate the services they wish to use on a case-by-case basis to ensure that FERPA requirements are met (US Department of Education, 2014).

Moreover, 'FERPA does not directly apply to private-sector data brokers and some student data types fall outside of FERPA's scope' (Russell et al, 2018). Certain information (including the student's name, date and place of birth, major field of study, dates of attendance, degrees and awards received) may be disclosed without prior written consent (unless parents or students have opted out). There are also a number of exceptions whereby school officials can disclose information from students' records to

[32] The Global Privacy Assembly, previously International Conference of Data Protection and Privacy Commissioners, is a long-established global forum counting over 130 data protection and privacy authorities exchanging best practices and undertaking common initiatives. The DEWG was established in 2013 and has expanded to 67 DPA members from across the world.

[33] See https://iite.unesco.org/publications/personal-data-and-privacy-protection-in-online-learning/

outside providers 'in lieu' of parental consent, for the pursuit of legitimate educational services. Service providers to schools such as 'PowerSchool, Clever, Google Apps for Education, and the inexpensive Chromebook laptops' have been recognized 'as authorized representatives of the schools they serve' and as such, allowed to receive students' records (Francis & Francis, 2018).

California's Student Online Personal Information Protection Act (SOPIPA), which took effect in 2016, was the first of its kind to directly address how online education service providers collect and use student data. The scope of the Act does not include all learners, but is limited to websites, services or applications 'used primarily for K–12 school purposes and […] designed and marketed for K–12 school purposes.' It expressly does not apply 'to general audience Internet Web sites, general audience online services, general audience online applications, or general audience mobile applications'. Personal information goes beyond the classic attributes, to include 'text messages, […], search activity, photos, voice recordings, or geolocation information'. The law forbids the EdTech service operator to use information acquired through the learner's use of its services for targeted advertising purposes, either on its own service or any other online service. The law also prohibits selling of students' information and profiling of students, but it allows the use of data for personalized learning. SOPIPA has been referred to as a model to govern education service providers' collection and use of education data for states across the country. Between 2015 and 2018, across the USA, 'states have introduced 109 bills and passed 24 new laws based on the SOPIPA model' (Data Quality Campaign, 2018).

Inherent limitations of self-regulatory initiatives

The major actors in online education are technology companies, and it is essential that they respect the human right to privacy. States can, by law, require compliance by the private sector with privacy standards. Aside from the public regulatory efforts, non-State actors have engaged in voluntary self-regulatory initiatives. A core weakness of these, however, is the apparent conflict between some of their commitments and their core interests and business model.

Both 'soft law' endeavours such as the United Nations' Guiding Principles on Business and Human Rights (UNGP), or industry initiatives such as the Global Network Initiative (GNI), have sought to impose human rights obligations and social responsibility upon non-State actors. The UNGP of 2011 provides 'a set of principles that states and businesses should apply to prevent, mitigate, and redress corporate-related human rights abuses' (Jørgensen, 2018: 255), including the right to privacy. However, the obligation for non-State actors to respect human rights in that framework remains a moral one, not a legal one. The GNI is an 'alliance of Internet and telecommunications companies, human rights and press freedom groups, investors, and academic institutions' whose members have committed 'to collaborate in the advancement of user rights to freedom of expression and privacy'.[34] The main feature of this endeavour is that it is based on a voluntary approach, which raises questions about its effectiveness. Jørgensen notes that there is an obvious paradox in expecting 'that the boundaries for data collection and use will be most effectively protected by companies whose business model is built around harnessing personal data as part of their revenue model'. One can expect companies to 'push back against illegitimate government requests for user data', but they are less likely to restrain their own practices when they are so fundamental to their core activities. (Jørgensen, 2018).

EdTech providers voice their commitment to protect the privacy of their users. These commitments can sometimes take the form of a collective pledge, or individual statements on their own platforms. When such pledges mention their compliance with existing national regulations, these are 'tokens' of their obedience to requirements to which they are bound by law. But when their commitment to data protection goes beyond legal requirements, pledges then become cases of self-regulation, marked by their voluntary nature. As already highlighted, the conflicting nature of the interests at stake calls into question the reliability of such promises.

In the United States, the Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA) designed a Student Privacy Pledge 'to safeguard student privacy regarding the collection, maintenance, and use of student personal information'.[35] The signatories are committed, among other things, not to sell student personal information nor use or disclose student information collected through an educational/school service for behavioural targeting of advertisements or profiling (Student Privacy Pledge, n.d.). However, a number of signatories to the Pledge have come under scrutiny for alleged violation of their promises in the Pledge (as well as of binding legal provisions), as well for showing inadequate security measures for the protection of student data (Pfeffer-Gillett, 2018). Analysis of a limited sample of signatories' privacy policies and terms of service against the commitments made in the Pledge reveal a number of potential noncompliance issues. This suggests that for some of the participating EdTechs, adhering to the Pledge means little more than 'paying lip service to its goals' (Pfeffer-Gillett, 2018). Also, it should be noted that the definition that the pledge gives of a 'student' applies to students in United States' elementary and secondary schools and does not include learners on Internet education platforms outside of that limited scope.

[34] See https://globalnetworkinitiative.org/
[35] See https://studentprivacypledge.org

Privacy by design

Technology can contribute to better privacy and security – including that of students – by the way it is designed and incorporates control and restriction options in the operations performed on data as it is being collected and processed. This is commonly referred to as the 'privacy by design' and/or 'security by design' approach. Privacy by design is an approach which was first developed by former Ontario Privacy Commissioner Dr. Ann Cavoukian in the 1990s, who advanced 'the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation' (Cavoukian, n.d.).

One of the first solutions that this movement advocated was the deployment of Privacy-Enhancing Technologies (PETs) (Cavoukian, n.d.), though the approach now has a more holistic reach, also looking at the organizational measures for data processing. The most often-cited examples of PETs would be encryption and pseudonymization. There is a groundswell of interest in how the design of technologies, which is not neutral, contributes to shaping the perceptions, behaviours and values of technology users: 'design is power because people react to design in predictive ways' (Hartzog, 2018: 34). The 'signals and transaction costs generated by design' are elements that support users in trusting other people. Design should 'prioritize control where it is most important and useful without becoming a burden' (Hartzog, 2018: 95).

The report of the Broadband Commission Working Group on Digital Skills for Life and Work mentions several applications developed to support individual users in their critical understanding 'of the data implications of their technology use' (Broadband Commission, 2017). One of those is Mozilla's Lightbeam add-on for its Firefox web browsers, which uses 'interactive visualizations' to show the relationships between visited websites and third parties to which they are providing information.[36] Other browser add-ons (such as Privacy Badger) work as advertisement-blocking extensions, stopping the tracking of users' online activities by advertisers and other third-party trackers.[37] The French Commission Nationale de l'Informatique et des Libertés (CNIL) published a recommendation to provide specific safeguards to protect the interests of the child, which should also result in the implementation of specific protection measures, by and on the websites, services and applications that children are likely to use, from the conception stage (CNIL, 2021).

The education sector has seen nascent certification initiatives. In the United Kingdom, an EdTech supplier self-certification scheme was put in place in 2014 and enabled 'providers to confirm their compliance with the key principles and requirements of the DPA' (Data Protection Act) (UK Department of Education, 2014). The Internet Keep Safe Coalition (iKeepSafe) has established a digital products' certification programme, attesting to EdTechs' compliance with State and federal requirements for handling protected personal information. Different certifications exist: FERPA certified, COPPA Safe Harbour Certified, California Student Privacy Certified, etc. Beyond product assessments, regular monitoring and training support is also offered. Common Sense, a US-based NGO, has set up a review programme of EdTech tools that are reviewed, evaluated[38] and rated on their security and privacy practices.[39] The evaluation process breaks down the product's overall score into several categories of 'concern': data collection, data sharing, data security, data rights, data sold, data safety, advertisements and tracking, parental consent and school purpose. Such programmes are helpful for learners, parents, educators and employers, in guiding their choices and decisions regarding the tools they want to work with. Ministries of Education can explore official certification programmes according to their own legal context.

Empowering learners and educators with relevant digital literacy skills

SDG target 4.4 aims to 'substantially increase the number of youth and adults who have relevant skills, including technical and vocational skills, for employment, decent jobs and entrepreneurship'.

The target is broad, but the associated skills indicators (4.4.1. and 4.4.2.) focus on ICT skills and digital literacy skills. A task force established by the Global Alliance to Monitor Learning and chaired by the Global Education Monitoring (GEM) Report has been working on defining and developing indicator 4.4.2: 'the percentage of youth and adults who have achieved at least a minimum level of proficiency in digital literacy skills'. The taskforce proposes the following definition for Digital Literacy Skills:

> Digital literacy is the ability to define, access, manage, integrate, communicate, evaluate and create information safely and appropriately through digital technologies and networked devices for participation in economic and social life. It includes competences that are variously referred to as computer literacy, ICT literacy, information literacy, data literacy and media literacy (UIS, 2018: 132).

[36] See https://addons.mozilla.org/en-US/firefox/addon/lightbeam/
[37] See https://privacybadger.org/#What-is-Privacy-Badger
[38] See https://privacy.commonsense.org/resource/full-evaluation-questions
[39] See https://www.commonsense.org/education/search?contentType=reviews

In the UIS-led process of establishing a global framework to guide the development, monitoring and assessment of digital literacy skills, the digital literacy frameworks of 47 countries were reviewed, identifying two types: frameworks developed at the national or sub-national level and frameworks used by commercial enterprises for training courses and assessment (UIS, 2018). A comparative study selected six of the national frameworks (Costa Rica, India, Kenya, Philippines, Chile and British Columbia (Canada)) and three enterprise frameworks to map onto the European DigComp 2.0 framework. It found that one of the most frequently valued digital literacy competences was that of 'protecting personal data and privacy'. The proposed Digital Literacy Global Framework includes competences around digital safety, such as protecting devices and protecting personal data and privacy (UIS, 2018).

Table 1: Proposed competence area number 4 and competences for the Digital Literacy Global Framework

Competence area and competences		Description
Competence area 4: Safety		To protect devices, content, personal data and privacy in digital environments. To protect physical and psychological health, and to be aware of digital technologies for social well-being and social inclusion. To be aware of the environmental impact of digital technologies and their use.
4.1	Protecting devices	To protect devices and digital content, and to understand risks and threats in digital environments. To know about safety and security measures and to have due regard to reliability and privacy.
4.2	Protecting personal data and privacy	To protect personal data and privacy in digital environments. To understand how to use and share personally identifiable information while being able to protect oneself and others from damages. To understand that digital services use a 'privacy policy' to inform how personal data is used.
4.3	Protecting health and well-being.	To be able to avoid health risks and threats to physical and psychological well-being while using digital technologies. To be able to protect oneself and others from possible dangers in digital environments (e.g. cyber bullying). To be aware of digital technologies for social well-being and social inclusion.
4.4	Protecting the environment	To be aware of the environmental impact of digital technologies and their use.

Source: UIS, 2018, p.24. Available under CC BY SA 30. IGO

The GPA has been active for a number of years in voicing the need to raise children's awareness of the privacy implications of their online behaviours, and to include data protection issues among digital literacy education. In 2008, its Resolution on Children's Online Privacy (ICDPPC, 2008) called for educators to include privacy education in their curricula. Also in 2016, the GPA recommended that data protection and privacy education would be included in study programmes and curricula, and that educators would be offered training on data protection and privacy (ICDPPC, 2016a). In this regard, the Assembly adopted an international competency framework for school students on data protection and privacy (ICDPPC, 2016b). The GPA's DEWG has since been monitoring related countries' activities. In 2019, it sent out a survey to Data Protection Authorities (DPA) on the approaches adopted by countries to integrating the competency framework into school curricula. Based on responses from 14 DPAs, it provided a summary of concrete adaptations, including curriculum reform efforts in Canada, France and Mexico (ICDPPC, 2019).

When the GPA adopted its international competency framework for school students on data protection and privacy, it stressed that training the educators was a significant pillar of the efforts to pass on skills to the students, and that there was a lack of existing training in this regard. It therefore called for the competency framework to be used not only as a tool for teaching students, but for training the educators as well (ICDPPC, 2016a). In its follow-up monitoring activities, the GPA DEWG has been mapping new initiatives regarding teacher training. In 2017, it reported that a number of countries (France, Luxembourg, Albania, Mexico and Senegal) were conducting training modules targeting teachers and school directors, as well as establishing partnerships with university and/or national education training institutes to further develop training modules for future teachers on fundamental data protection principles (ICDPPC, 2017). In 2019, it also reported that data protection training programmes were being developed for educational actors in the public and/or private sector by Mexico, Philippines, Czech Republic, Poland and Burkina

Faso (ICDPPC, 2019). Each year, the DPAs share with the GPA new educational modules, games and other pedagogical guides for children, teenagers and educators.[40]

Box 12: The Gender Skills Gap

While privacy breaches can have a stronger impact on some people such as girls and women, LGBTQIA+ individuals or marginalized groups, the possibility for such breaches is higher when people do not have sufficient digital skills and are unaware of the value of their personal data. This is particularly important considering the gender gap in digital skills that exists, especially for girls and women. In a study conducted across 10 low- and middle-income countries, women were 1.6 times more likely than men to report lack of skills as a barrier to Internet use (World Wide Web Foundation, 2015). This gap is present across the entire skills spectrum, from the lowest skills proficiency levels, such as using devices and Internet access to their full potential, to the most advanced ones, such as computer programming (EQUALS and UNESCO, 2019). It is cross-regional but is more pronounced for women who are older, less educated, poor, or living in rural areas and developing countries (Ibid.).

Support structures and resources for education policy-makers and teachers

Ministries of Education and education institutions are increasingly in need of internal resources to help them support their educators and ensure that they are legally compliant. The US Department of Education has a dedicated Student Privacy Policy Office (SPPO) that is responsible for administering and enforcing federal laws relating to the privacy of students' education records, and for providing policy and guidance. The SPPO has also hosted a Privacy Technical Assistance Center (PTAC) since 2010. As previously mentioned, the GDPR requires any public body processing personal data to assign a Data Protection Officer (DPO) to be in charge of ensuring compliance by the institution with GDPR provisions, by monitoring the organization's policies, overseeing audits, etc.

Ministries of Education release guidelines to accompany the development of online education. The US PTAC, for example, published a guidance document in 2014, 'Protecting student privacy while using online educational services: requirements and best practices' (U.S. Department of Education, 2014). The UK Department for Education has provided local authorities, school leaders, school staff and governing bodies with advice on Cloud software services taking account of the Data Protection Act (UK Department of Education, 2014), as well as a toolkit for schools to help them with data protection activity, including compliance with the GDPR (UK Department for Education, 2018). The Ministry of Education of the People's Republic of China published a guidance document on the development of online education in 2019, including 'measures to establish a standardized online education system to safeguard personal information security for teachers and students' (OneTrust Data Guidance, 2019b). In France, the Ministry of Higher Education issued a form on monitoring and education during the COVID-19 crisis. It draws the attention of educational institutions to the fact that using the services of distance evaluation providers leads to processing of personal data (including photos and videos) that should be recorded by the DPO in the register of processing activities. It also calls on education institutions to ensure that the providers they contract meet the legal requirements in terms of privacy and security practices (Ministère de l'enseignement supérieur, de la recherche et de l'innovation, 2020). Further guidelines and codes of conduct have been developed recently by States, including in education, as documented by the GPA.[41]

Because education, including through digital and hybrid learning, online tools, platforms and LMS, increasingly captures student learning and achievement data, educators are also expected to analyse the data, applying it to their existing knowledge of their students, and adjusting their teaching and planning based on the data analytics derived from it. Educators must know how to use student data to identify gaps in concept and skills acquisition, areas for remediation or enrichment, and patterns that affect groups of learners and the entire cohort. Educators must also know how to protect their learners' data privacy and security, how and where to store data and the risks related to the tools they use in teaching and learning, assessment and sharing of information regarding their students.

Because of their expertise in this area, data protection and privacy authorities can provide help and support to educators, including by publishing guidelines and toolkits. A few examples are provided below:

[40] See https://globalprivacyassembly.org/news-events/gpa-awards/education-public-awareness/#A1

[41] See GPA, Digital Education Working Group Report – October 2020 (final 20201013), pp-38-39. Available at: https://globalprivacyassembly.org/wp-content/uploads/2020/10/DEWG-2019-2020-Annual-Report-GPA-20200921-finalannexes_Oct-2020_final-en-211020-1.pdf

Australia's Office of the Safety Commissioner is located within the Australian Communications and Media Authority and is a different body from the Data Protection Authority of the country (the Office of the Australian Information Commissioner). However, its role is to promote online safety for all Australians, and in that capacity it has put together an eSafety Toolkit for Schools (Australian Government, eSafety Commissionner, n.d.). The toolkit is designed to support schools in creating safer online environments, and includes, among other documents, a set of guidelines for social media use, video sharing and online collaboration. In the COVID-19 context, Canada's Office of the Information and Privacy Commissioner of British Columbia (Canada) has issued a guidance document for educators on choosing online learning tools in compliance with the Protection of Privacy Act (OIPC, 2020). A code of practice for online services focusing on age-appropriate design has been published by the UK Information Commissioner's Office (n.d.). The Gibraltar regulatory authority's Information Commissioner has developed educational resources, including for teachers to equip them for educating students on privacy and data protection. Two packs (one for middle schools and one for secondary schools) have been published and include lessons plans and resources based on the GPA international competency framework.[42] The French CNIL published guidelines for education institutions and parents when using online tools from private providers[43] as well as advice on monitoring online exams.[44]

In addition to resource documents, data protection and privacy authorities can also provide advice. In May 2020, the Hellenic Data Protection Authority issued an opinion on the provision of remote education in the context of COVID-19 and found it to be lawful:

> The Opinion highlights that the purpose of providing education constitutes a lawful basis for the processing of personal data, and that a Data Protection Impact Assessment ("DPIA") will be required to ensure the appropriate assessment of risks and the implementation of measures to mitigate them. In addition, the Opinion states that, after the publication of a ministerial decision on remote education, it will be possible to assess the compatibility of remote education with data protection legislation. (OneTrust Data Guidance, 2020c).

In 2017, the GPA DEWG circulated a survey among the Assembly's members with a view to gathering information about their experiences with educational service platforms. One of its questions asked whether data protection and privacy authorities were consulted for advice on the compliance of educational online platforms with their data protection regulations. Twenty-one out of 33 respondents answered positively. The requests arose from parents, parent and/or teacher associations and service providers, and addressed a variety of issues, such as 'the recording of absences in google docs, (…) the use of Skype in distance learning, (…) requirements for consent and notice with parents, (…) visibility of personal data on the platform'. They also enquired about the compliance of platforms in general, 'such as Microsoft Office 365, myschool (https://myschool.sch.gr/), Apple School, and G-suite for education', and some were asked for product recommendations and assessment tools (ICDPPC, 2017).

Relevant international organizations have contributed to supporting privacy and security of learners' data by publishing technical guides and handbooks. As with regulatory frameworks, few are specific to online learning, and most of them focus on protecting children online. This includes work by the Council of Europe,[45] the ITU,[46] the Broadband Commission,[47] the OECD[48] and UNICEF.[49] The UNESCO Institute for Information Technologies in Education (UNESCO IITE) recently published a technical guide to ensure the security of personal data specifically for online education platforms (UNESCO IITE, 2020), while the Global Privacy Assembly's Digital Education Working Group (DEWG) is monitoring the implementation of its 2018 resolution on e-learning platforms and working on an upcoming inventory of Recommendation Guides and Codes of Practice for online learning platforms (ICDPPC, 2019). With Open Source, educational institutions own their software, meaning privacy is inherent in the design of the system. The technology keeps the data at the local level. Learners' traces are contained within the educational institutions, not centralized or stored on Cloud infrastructures.

An Open EdTech Association[50] was also recently set up. The aim is to promote and support the idea that formal education should be able to own its own infrastructure, not just rent it (and hand over ownership of the data to the infrastructure's owner).

[42] See https://www.gra.gi/dataprotection/public-awareness/resources-for-teachers

[43] See https://www.educnum.fr/fr/outils-de-la-continuite-pedagogique-les-conseils-de-la-cnil

[44] See https://www.cnil.fr/fr/surveillance-des-examens-en-ligne-les-rappels-et-conseils-de-la-cnil

[45] The Digital Citizenship Education Handbook: Being a Child in the Age of Technology, published in April 2019 by the Education Policy Division (Council of Europe, 2019), as well as the Recommendation to Member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, adopted by the Committee of Ministers (Council of Europe, 2018a).

[46] Guidelines on Child Online Protection (ITU, 2016).

[47] The Broadband Commission has established a Working Group on Child Online Safety, which has published a report in 2019 (Broadband Commission, 2019).

[48] In the framework of its work revising its Recommendation on the protection of children online, the OECD considered policy and legislative avenues for countries to explore, in a dedicated chapter of a 2019 publication (Burns & Gottschalk, 2019).

[49] The organization published an industry toolkit for protecting children's online privacy and freedom of expression (UNICEF, 2018). It is also working on developing a manifesto to protect children's data security and privacy (Manifesto for good governance of children's data) and has launched a project to explore approaches to protecting and upholding child rights in an evolving AI world (AI for children).

[50] See https://openedtech.global

Towards an education data privacy ecosystem

The education sector's response to digitization has been varied over the last few decades, including during the COVID-19 pandemic. Some sectors, notably with non-formal and informal offerings, have embraced this fast-paced transition, while others, notably basic education and TVET systems with formal offerings, have been much slower in their responses to both the opportunities and the risks associated with digitization.

This publication has attempted to provide the international education and training community with a current view of this situation, juxtaposing the pivotal role of data privacy with the centrality of the learner in the lifelong learning discourse. It argues very strongly that there is an urgent need to develop and implement protective frameworks to enforce the protection of learners' data through 'privacy by design' approaches and the development of international rules of engagement. Building on consultations with experts, networks and Member States, the Education Sector of UNESCO is mobilizing this policy dialogue.

In the spirit of the COVID-19 Global Education Coalition launched by UNESCO, the Organization will pursue further partnerships and set up an expert group to work on international tools around the privacy and security of learners' data. Links with related initiatives will be explored. These include UNESCO's work on data analytics in education and on achieving SDG4, and the Recommendation on the Ethics of Artificial Intelligence. Through the work of UNESCO and its partners, the foundation is being laid for an education data privacy ecosystem that draws together international thinking across five main vectors: data protection as a fundamental human right; data for individualized learning experiences and identity; privacy by design; privacy as trust; and data as a driver of better policy in education and training. These vectors are far from fully developed, nor have they been agreed internationally. They do, however, represent an important thrust that UNESCO hopes will gain momentum as they are refined in the coming months and years. Each of these vectors is briefly described below.

Data protection as a fundamental human right

With the emergence of powerful data mining processes and analytics, technology can aggregate and integrate data to draw far-reaching inferences about individuals' capacities and profiles. Currently, the UN framework does not recognize personal data protection as a fundamental right. By contrast, the right to privacy is a long-established right. UNESCO plans to work with key partners across the public and private sectors to promote this thinking, and ultimately to put in place an internationally agreed normative instrument to recognize personal data protection as a human right.

Data for personalized learning experiences and identity

Data is able to capture the full learning experience of individuals and connect it to other areas of human activity including work, health and leisure. Data analytics can offer personalized, adaptive and flexible learning processes and pathways, an enhanced ability to evaluate the multiple dimensions of learners' competencies, and better-informed education decision-making. In this wider sense, learners' digital identity is a version, or facet, of a person's social identity that can be used to facilitate mobility, recognition of credentials and transferability of learning records across ecosystems. UNESCO aims to play a greater role in setting the agenda in terms of the methodologies and ethical principles to be applied both by public and private institutions managing digital identities and individual learning data (UNESCO, 2022b). For facilitating mobility of learners, cross-border recognition of learning experiences and outcomes and interoperability of ecosystems, UNESCO can eventually facilitate a global exchange network to enable Member States' recognized authorities to share learning records and preserve privacy and security.

Privacy by design

The education sector has traditionally been mindful of the rights of young learners, but less so of the vulnerability of lifelong learners directly associated with their personal data. New privacy laws have gained traction across the globe, and their application and interpretation within education settings requires more attention. UNESCO aims to play a role in these processes, with a strong emphasis on the development of 'privacy by design' education systems and policies.

Privacy as trust

A distinguishing feature of the way students behave in an educational context and share their personal information is that they inherently trust their education providers. The educational context is supposed and considered to be a safe environment. UNESCO argues that education providers and data processors in the educational context should be considered as personal information fiduciaries. By initiating work to outline the legal implications of such a status, UNESCO aims to compel relevant actors to behave in compliance with standards of trustworthiness and encourage national systems to enforce such a normative framework in their legal systems.

Data as a driver of better policy in education and training

Leveraging data analytics and AI for better policy is in its infancy in the education sector. While developed economies are investing massively in data industries, including for social sectors such as health and education, low-income countries run the risk of being left behind, creating a widening gap between those who reap the benefits of this new data-driven world and those who do not (UNESCO 2021). The lack of institutions with the requisite administrative capacity, decision-making autonomy and financial resources limits the real advantage of data for decision-making. In some contexts, the demand for, and the culture of, data-informed decision-making are also lacking. UNESCO should provide policy advice and technical assistance to its Member States. UNESCO should build on its comparative advantages to fulfil its mandate as an honest broker and the go-to source of education data and evidence. It should lead the debate on the right to data protection in the education and training context.

As a first step towards tangible international guidelines for data privacy in education, UNESCO plans to further develop these five vectors in collaboration with the broader education data privacy ecosystem. These players include the UIS and many other UN agencies working in education, as well as new strategic partnerships to acquire capabilities in data collection, storage and processing made possible through key members of the Global Education Coalition to leverage expertise and delivery capacity.

This ecosystem comprises many new aspects that in the recent past might have been merely tangential to the education system. Examples include the emerging regional normative frameworks, such as the European GDPR, but also many national data protection policies and the associated data protection authorities and the roles they are introducing, including data protection officers. We trust that this publication will not only encourage debate on data privacy in education but will lead to meaningful and urgent steps to protect the data rights of lifelong learners during the COVID-19 pandemic, and into the increasingly digital future that lies ahead.

Bibliography and references

Accredible. (2018). *A comprehensive guide to digital badges*. Available at: https://www.accredible.com/wp-content/uploads/2018/07/A-Comprehensive-Guide-to-Digital-Badges-Accredible.pdf

Acquisiti, A., Taylor, C. and Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), pp. 442–492. Available at: http://dx.doi.org/10.1257/jel.54.2.442

African Union. (2014). *Convention on Cyber Security and Personal Data Protection*. Available at http://www.worldlii.org/int/other/IDPrivAgmt/2014/1.html

Aldowah, H., Al-Samarraie, H. and Fauzy, W.M. (2019). Educational data mining and learning analytics for 21st century higher education: A review and synthesis. *Telematics and Informatics*, Vol. 37, pp. 13-49. Available at: https://doi.org/10.1016/j.tele.2019.01.007

ALECSO and ITU Arab Regional Office. (2016). *Guidelines to improve the use of the Cloud Computing Technology in Education in Arab Countries.* Available at: http://www.alecso.org/newsite/images/2016files/isdarat/Cloud-guidelines-Alecso-Final.pdf

Altman, M., Wood, A., O'Brien, D.R. and Gasser, U. (2018). Practical approaches to big data privacy over time. *International Data Privacy Law,* 8(1), pp. 29–51. Available at: https://doi.org/10.1093/idpl/ipx027

Angwin, J. and Parris, T. (2016). *Facebook Lets Advertisers Exclude Users by Race.* Available at: https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

Angwin, J. and Tobin, A. (2017). *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*. Available at: https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin

Angwin, J., Scheiber, N. and Tobin, A. (2017). *Dozens of Companies Are Using Facebook to Exclude Older Workers From Job Ads.* Available at: https://www.propublica.org/article/facebook-ads-age-discrimination-targeting

APEC. (2015). *APEC Privacy Framework*. Available at: http://www.worldlii.org/apec/other/APECPrivLRes/2005/1.html

Australian Government. eSafety Commissionner. (n.d.) *eSafety Toolkit for Schools*. Available at: https://www.esafety.gov.au/educators/toolkit-schools

Barth, S. and de Jong, M.D.T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, Vol. 34, Issue 7, pp. 1038-1058. Available at: https://doi.org/10.1016/j.tele.2017.04.013

Bellovin, S. M., Blaze, M., Landau, S. and Pell, S.K. (2016). It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law. *Harvard Journal of Law and Technology*, Forthcoming. Available at https://ssrn.com/abstract=2791646

Bourtoule et al. (2020). Machine Unlearning. *42nd IEEE Symposium of Security and Privacy.* Available at: https://doi.org/10.48550/arXiv.1912.03817

Bridges, K.M. (2017). *The Poverty of Privacy Rights*. Stanford, Stanford Law Books.

BrightBytes. (n.d.). *The Digital Privacy, Safety & Security Module.* Available at: http://www.brightbytes.net/digitalprivacy/

Broadband Commission. (2017). *Working Group on Education: Digital skills for life and work*. Available at http://www.broadbandcommission.org/Documents/publications/WG-Education-Report2017.pdf

Broadband Commission. (2019). *Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online*. Available at: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf

Brunner, L. (2018). Digital Communications and the Evolving Right to Privacy. In M. Land and J. Aronson (eds.), *New Technologies for Human Rights Law and Practice*, pp. 217-242. Cambridge, Cambridge University Press. doi:10.1017/9781316838952.010

Burns, T. and Gottschalk, F. (dir. pub.) (2019). Educating 21st Century Children: Emotional Well-being in the Digital Age, *Educational Research and Innovation*, Éditions OCDE, Paris, Available at: https://doi.org/10.1787/b7f33425-en

Cavoukian, A. (n.d.). *Privacy by Design. The 7 Foundational Principles.* Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Chiavetta, R. (2018). *The road to GDPR certifications won't be a short one, it seems.* Available at: https://iapp.org/news/a/the-road-to-seeing-gdpr-certifications-wont-be-a-short-one/#

Chignard, S. (2013). A brief history of Open Data. *Paris Innovation Review.* Available at: http://parisinnovationreview.com/articles-en/a-brief-history-of-open-data

CISCO. (2018). *Cisco Global Cloud Index: Forecast and Methodology, 2016–2021. White Paper.* Available at: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf

CNIL. (2021). *Recommandation 8: prévoir des garanties spécifiques pour protéger l'intérêt de l'enfant*. Available at: https://www.cnil.fr/fr/recommandation-8-prevoir-des-garanties-specifiques-pour-proteger-linteret-de-lenfant

Collins, A. (2017). *Four reasons to question the hype around blockchain.* Available at: https://www.weforum.org/agenda/2017/07/four-reasons-to-question-the-hype-around-blockchain

Committee on the Rights of the Child (CRC). (2018). *Concept Note for a General Comment on children's rights in relation to the digital environment.* Available at: https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/CN.docx

Commonwealth of Learning. (2020). *Open and Distance Learning: Key Terms and Definitions.* Available at: http://hdl.handle.net/11599/3558

Council of Europe. (2014). *Recommendation of the Committee of Ministers to Member States on a Guide on Human Rights for Internet Users.* Available at: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2014-6-of-the-committee-of-ministers-to-member-states-on-a-guide-to-human-rights-for-internet-users-adopted-by-the-committee-of-?inheritRedirect=false&desktop=true

Council of Europe. (2018a). *Recommendation of the Committee of Ministers to Members States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.* Available at: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

Council of Europe. (2018b). *Convention 108 +. Convention for the protection of individuals with regard to the processing of personal data.* Available at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

Council of Europe. (2019). *Digital Citizenship Education Handbook: Being a Child in the Age of Technology. Council of Europe Publishing: Strasbourg.* Available at: https://rm.coe.int/168093586f

Council of Europe. (2021). *Children's data protection in an education setting. Guidelines. Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data. Convention 108.* Available at: https://edoc.coe.int/fr/les-enfants-et-l-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html#

Cox, J. (2017). *Hacker Steals Millions of User Account Details from Education Platform Edmodo.* Available at: https://motherboard.vice.com/en_us/article/ezjbwe/hacker-steals-millions-of-user-account-details-from-education-platform-edmodo

Credly. (2019). *Shifting The Up-Skilling Paradigm. Digital badges help IBM create a diverse, inclusive workforce.* Available at: https://resources.credly.com/resources/case-study-ibm

Data Quality Campaign. (2018). *Education Data Legislation Review.* Available at: https://2pido73em67o3eytaq1cp8au-wpengine.netdna-ssl.com/wp-content/uploads/2018/09/2018-DQC-Legislative-Summary.pdf

Data Revolution Group (2014). *A world that counts: Mobilising the data revolution for sustainable development*. Report prepared at the request of the United Nations Secretary-General, by the Independent Expert Advisory Group on a Data Revolution for Sustainable Development. Available at: https://www.undatarevolution.org/wp-content/uploads/2014/11/A-World-That-Counts.pdf

Donovan, J., Caplan, R., Matthews, J. and Hanson, L. (2018). Algorithmic Accountability: A Primer. *Data & Society.* Available at https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL.pdf

Economic Community of West African States (ECOWAS). (2010). *ECOWAS Supplementary Act on Personal Data Protection,* A/SA.1/01/10, Abuja, 16 February 2010. Available at: https://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf

Edmodo. (n.d.). *Why Am I Seeing This Sponsored Post?* Available at: https://support.edmodo.com/hc/en-us/articles/115000999288-Why-Am-I-Seeing-This-Sponsored-Post-

Eichensehr, K. (2017). *Data Extraterritoriality.* UCLA School of Law, Public Law Research Paper No. 17-24. Available at SSRN: https://ssrn.com/abstract=3009774

Eight principles of open government data. (2007). Available at: https://opengovdata.org

Electronic Frontier Foundation. (2017). *Spying on Students: School-Issued Devices and Student Privacy.* Available at https://www.eff.org/files/2017/04/13/student-privacy-report.pdf

European Commission. (2016). EU-U.S. *Privacy Shield Factsheet.* Available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

European Commission. (n.d.). *What does data protection 'by design' and 'by default' mean?* Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en

European Commission. (2018a). *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law.* Available at https://ec.europa.eu/info/sites/info/files/independent_study_on_automated_decision-making.pdf

European Commission. (2018b). *News. Cybersecurity Act*. Available at: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

European Commission. (2020). *Digital Economy and Society Index (DESI) 2020.* Thematic chapters. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67086

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) *Official Journal of the European Union*, Vol. L119 (4 May 2016), pp. 1-88, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

European Union. (2017). *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017)477*, Available at: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

Eurostat. (2018). *Digital economy & society in the EU — a browse through our online world in figures.* Available at: https://ec.europa.eu/eurostat/cache/infographs/ict/index.html

Experience API. (n.d.a). *What is the Experience API?* Available at: https://xapi.com/overview/

Experience API. (n.d.b). *The Enterprise Learning Ecosystem*. Available at: https://xapi.com/ecosystem/

Fain, P. (2019). IBM Looks Beyond the College Degree. *Inside HigherEd*. Available at: https://www.insidehighered.com/digital-learning/article/2019/10/29/interview-ibm-official-about-companys-new-collar-push-look

Fitzgerald, B. (2017). *Tracking of teachers and students in Edmodo.* Available on: https://archive.funnymonkey.com/2017/tracking-of-teachers-and-students-in-edmodo.html

Fitzgerald, B. (2018). *Fordham CLIP Study on the Marketplace for Student Data: Thoughts and Reactions*. Available at: https://funnymonkey.com/2018/fordham-clip-study-on-the-marketplace-for-student-data-thoughts

Forbes. (2018). *Advancing a culture of education at IBM.* Available at: https://www.forbes.com/sites/deniselyohn/2018/09/12/advancing-a-culture-of-education-at-ibm/#7098aae45265

Foreseman, B. (2020). *Students say Florida State's online exam tech violates privacy*. Available at: https://edscoop.com/students-say-florida-states-online-exam-tech-violates-privacy/

Francis, L. P. and Francis, J. G. (2017). *Privacy. What everyone needs to know.* New York, Oxford University Press.

Future of Privacy Forum and Actionable Intelligence for Social Policy. (2018). *Nothing to hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems*. https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf

Future of Privacy Forum. (2020). Privacy 2020: *10 privacy risks and 10 privacy enhancing technologies to watch in the next decade.* Available at: https://fpf.org/wp-content/uploads/2020/01/FPF_Privacy2020_WhitePaper.pdf

G20 Education Working Group. (2021). *Report on blended education and educational poverty. Version II.* https://unesdoc.unesco.org/ark:/48223/pf0000380190/PDF/380190eng.pdf.multi

Gellman, R. (2019). *Fair Information Practices: A Basic History, Version 2.19.* https://bobgellman.com/rg-docs/rg-FIPshistory.pdf

Global Privacy Assembly. (2021a). *Adopted Resolution on children's digital rights.* Available at: https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Childrens-Digital-Rights-Final-Adopted.pdf

Global Privacy Assembly. (2021b). *Policy Strategy Working Group 1: Global frameworks and standards.* Available at: https://globalprivacyassembly.org/wp-content/uploads/2021/10/1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf

Grech, A. and Camilleri, A. F. (2017). *Blockchain in Education.* Publications Office of the European Union. Available at: doi:10.2760/60649

Greenleaf, G. and Cottier, C. (2018). Data Privacy Laws and Bills: Growth in Africa, GDPR Influence. 152 *Privacy Laws & Business International Report*, pp. 11-13; UNSW Law Research Paper No. 18-52. Available at SSRN: https://ssrn.com/abstract=3212713

Greenleaf, G. (2019a). Global Tables of Data Privacy Laws and Bills (6th ed. January 2019). Supplement to 157 *Privacy Laws & Business International Report (PLBIR)*. Available at: https://ssrn.com/abstract=3380794

Greenleaf, G. (2019b) It's Nearly 2020, so What Fate Awaits the 1980 OECD Privacy Guidelines? (A Background Paper for the 2019 OECD Privacy Guidelines Review). 159 *Privacy Laws & Business International Report*, pp.18-21; UNSW Law Research Paper No. 19-42. Available at SSRN: https://ssrn.com/abstract=3405156

Greenleaf, G. (2019c). Global Data Privacy Laws 2019: 132 National Laws & Many Bills. 157 *Privacy Laws & Business International Report*, pp. 14-18. Available at: https://ssrn.com/abstract=3381593

Greenleaf, G. (2020). India's Data Privacy Bill: Progressive Principles, Uncertain Enforceability. 163 *Privacy Laws & Business International Report 1*, pp. 6-9. Available at: https://ssrn.com/abstract=3572620

Hartzog, W. (2018). *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, Harvard University Press.

Herold, B. (2017a). InBloom's Collapse Shines Spotlight on Data-Sharing Challenges. Available at https://www.edweek.org/ew/articles/2014/05/02/30inbloom.h33.html

Herold, B. (2017b). Popular Ed-Tech Platform Edmodo Hacked, Faulted for Ad-Tracking. Available at: https://blogs.edweek.org/edweek/DigitalEducation/2017/05/ed-tech_platform_edmodo_hacked_ad_tracking.html

Hillman, T., Bergviken Rensfeldt and A., Ivarsson, J. (2020). Brave new platforms: a possible platform future for highly decentralised schooling. *Learning, Media and Technology*, 45:1, pp. 7-16. Available at: DOI: 10.1080/17439884.2020.1683748

Ho, A. (2017). *Advancing Educational Research and Student Privacy in the "Big Data" Era.* Washington, DC, National Academy of Education. Available at: https://naeducation.org/wp-content/uploads/2017/05/Ho-FINAL.pdf

HTF Market Intelligence. (2019). *Global Virtual Schools Market 2019 by Company, Regions, Type and Application, Forecast to 2024.* Available at: https://www.htfmarketreport.com/reports/1636459-global-virtual-schools-market-5

Huntington, G. (2021). Cost Centres – Rethinking Legal Identity and Learning Vision. Available at: https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf

Ibero-American Data Protection Network (RIPD). (2017). *Standards for Personal Data Protection for Ibero-American States.* Available at: https://platform.dataguidance.com/sites/default/files/02.24.20_ibero-am_standards.pdf

IBM. (2019). *Annual Report*. Available at: https://www.ibm.com/annualreport/assets/downloads/IBM_Annual_Report_2019.pdf

International Conference on Data Protection and Privacy Commissioners (ICDPPC). (2008). *Resolution on Children's Online Privacy*. Available at: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Childrens-Online-Privacy-.pdf

ICDPPC. (2009). *International Standards on the Protection of Personal Data and Privacy.* Available at: http://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf

ICDPPC. (2016a). *Resolution for the Adoption of an International Competency Framework on Privacy Education.* Available at: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacy-education.pdf

ICDPPC. (2016b). *Personal Data Protection Competency Framework for School Students.* http://globalprivacyassembly.org/wp-content/uploads/2015/02/International-Competency-Framework-for-school-students-on-data-protection-and-privacy.pdf

ICDPPC. (2017). *Report of the International Working Group on Digital Education,* 2017. Available at: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Digital-Education-Working-Group-Report-1.pdf

ICDPPC. (2018). *Resolution on e-learning platforms.* http://globalprivacyassembly.org/wp-content/uploads/2019/03/dewg-resolution-adopted-20180918.pdf

ICDPPC. (2019). *Report of the International Working Group on Digital Education*, 2019. Available at: http://globalprivacyassembly.org/wp-content/uploads/2019/11/2018-2019-Activity-Report-V-final_DEWG_working-group-on-digital-education.EN_.August-2019.pdf

Internet Rights & Principles Coalition. (2018). *The Charter of Human Rights and Principles for the Internet.* Available at: http://internetrightsandprinciples.org/site/wp-content/uploads/2018/01/IRPC_english_5thedition.pdf

ITU. (2012). *Privacy in Cloud Computing. ITU-T Technology Watch Report*. Available at: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

ITU. (2016). *Guidelines for Children on Child online protection*. Available at: https://stisc-cert.gov.md/wp-content/uploads/2018/08/S-GEN-COP.CHILD-2016-PDF-E1.pdf

ITU. (2017). *ICT Facts and Figures 2017*. Available at https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf

Jarke, J. and Breiter, A. (2019). Editorial: the datafication of education. *Learning, Media and Technology*, 44:1, pp. 1-6. Available at: DOI: 10.1080/17439884.2019.1573833

Jason. (2017). *Open Data Anniversary: Ten Years after the Sebastopol Meeting.* Available at: https://www.opendatasoft.com/2017/12/07/open-data-anniversary-ten-years-sebastopol-meeting/

Joiner, M.C. (2018). To See or Not to See: The Constant Conflict Between Promoting Public Access to Information Whilst Maintaining Confidentiality in Student Records. *Southern University Law Review* 44. Available at https://ssrn.com/abstract=3132051

Jørgensen, R. (2018). Human Rights and Private Actors in the Online Domain. M. Land and J. Aronson (eds.), *New Technologies for Human Rights Law and Practice*, pp. 243-269. Cambridge, Cambridge University Press. doi:10.1017/9781316838952.011

Kelly, G., Graham, J. and Fitzgerald, B. (2018). 2018 State of Edtech Privacy Report, *Common Sense Privacy Evaluation Initiative.* San Francisco, CA, Common Sense. Available at: https://www.commonsense.org/education/sites/default/files/tlr-blog/cs-state-of-edtech-privacy-report.pdf

Koch, C. and Pieters, G.C. (2017). Blockchain Technology Disrupting Traditional Records Systems. *Financial Insights* - Dallas Federal Reserve Bank. Available at SSRN: https://ssrn.com/abstract=2997588

Livingstone, S., Stoilova, M. and Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. An evidence review*. London, London School of Economics and Political Science. Available at: http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review.pdf

Long, P. and Siemens, G. (2011). *Penetrating the fog: Analytics in learning and education*. Available at: https://er.educause.edu/articles/2011/9/penetrating-the-fog-analytics-in-learning-and-education

Macgilchrist, F., Allert, H. and Bruch, A. (2020). Students and society in the 2020s. Three future 'histories' of education and technology. *Learning, Media and Technology*, 45:1, pp. 76-89. Available at: DOI: 10.1080/17439884.2019.1656235

McKenzie, L. (2017). *E.U. Data-Protection Law Looms*, Available at: https://www.insidehighered.com/news/2017/11/06/eu-data-protection-law-looms

Microsoft Azure. (n.d.). *What is Cloud computing? A beginner's guide.* Available at: https://azure.microsoft.com/en-ca/overview/what-is-cloud-computing/

Ministère de l'enseignement supérieur, de la recherche et de l'innovation. (2020). *Fiche 6 – Evaluer et surveiller à distance*. Available at: https://services.dgesip.fr/fichiers/Fiche_6_-_Evaluer_et_surveiller_a_distance.pdf

Molnar et al. (2019). Virtual Schools in the U.S. 2019. *Boulder, CO: National Education Policy Center.* Available at: https://nepc.colorado.edu/sites/default/files/publications/Virtual%20Schools%202019.pdf

Mnkandla, E. and Minnaar, A. (2017). The Use of Social Media in E-Learning: A Metasynthesis. *The International Review of Research in Open and Distributed Learning,* 18(5). Available at: https://doi.org/10.19173/irrodl.v18i5.3014

Nassirian, B. (2017). *The General Data Protection Regulation Explained.* Available at: https://er.educause.edu/articles/2017/8/the-general-data-protection-regulation-explained

National School Board Association (NSBA). (2014). *Data in the cloud, A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era.* Available at: https://cdn-files.nsba.org/s3fs-public/Data_In_The_Cloud_Guide_NSBA_COSA_02-09-15.pdf?RQkKRotGvL6gD6tmH_jHZTHelMfxdlUA

Obrien, A. (2014). *A Starting Point for Ensuring Student Online Privacy.* Available at https://www.edutopia.org/blog/starting-point-ensuring-student-online-privacy-anne-obrien

OECD. (1997). *Recommendation of the Council concerning Guidelines for Cryptography Policy.* C(97)62/FINAL. Available at https://legalinstruments.oecd.org/en/instruments/115

OECD. (2012a). *Recommendation of the OECD Council on the protection of children online.* Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389%20

OECD. (2012b). *Assessment of Higher Education Learning Outcomes: Feasibility Study Report, Volume 1, Design and Implementation.* Available at: https://www.oecd.org/education/skills-beyond-school/AHELOFSReportVolume1.pdf

OECD. (2013). *Privacy Framework, including the 2013 Privacy Guidelines*. Available at http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

OECD. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being.* Paris, OECD Publishing. http://dx.doi.org/10.1787/9789264229358-en

OECD. (2019). Online activities. *Society at a Glance 2019: OECD Social Indicators. Paris, OECD Publishing.* Available at: https://doi.org/10.1787/205f8f17-en

OECD. (2020). Growing Up Online. *Addressing the Needs of Children in the Digital Environment.* Available at: https://www.oecd.org/sti/ieconomy/growing-up-online.pdf

OECD. (2021). *OECD Guidelines for Digital Service Providers.* Available at: https://legalinstruments.oecd.org/public/doc/272/5803627d-b49b-4894-8dbe-35f67fd10007.pdf

Office of the information and privacy commissioner for British Columbia (OIPC) (2016). *Investigation Report F16-01.* Available at: https://www.oipc.bc.ca/investigation-reports/1907

Office of the information and privacy commissioner for British Columbia (OIPC). (2020). *Guidance document for educators in choosing online learning tools in compliance with Protection of Privacy Act.* Available at: https://iapp.org/media/pdf/resource_center/fippa_online_learning_during_covid19.pdf

OneTrust DataGuidance and Future of Privacy Forum. (2019). *Comparing privacy laws: GDPR v. CCPA.* https://fpf.org/wp-content/uploads/2019/12/ComparingPrivacyLaws_GDPR_CCPA.pdf

OneTrust Data Guidance. (2019a). *Singapore: PDPC fines Marshall Cavendish SGD 40,000 for violating Section 24 of PDPA.* Available at: https://www.dataguidance.com/news/singapore-pdpc-fines-marshall-cavendish-sgd-40000-violating-section-24-pdpa

OneTrust Data Guidance. (2019b). *China: MoE releases guidance for developing online education.* Available at: https://www.dataguidance.com/news/china-moe-releases-guidance-developing-online-education

OneTrust Data Guidance. (2020a). *Québec: Ministry of Education and Higher Education announces data breach.* Available at: https://www.dataguidance.com/news/québec-ministry-education-and-higher-education

OneTrust Data Guidance. (2020b). *Norway: Datatilsynet fines Municipality of Oslo €120,000 for insufficient security in Skolemelding mobile app.* Available at: https://www.dataguidance.com/news/norway-datatilsynet-fines-municipality-oslo-€120000-insufficient-security-skolemelding-mobile

OneTrust Data Guidance. (2020c). *Greece: HDPA issues opinion on lawfulness of Ministry of Education remote education provision.* Available at: https://www.dataguidance.com/news/greece-hdpa-issues-opinion-lawfulness-ministry-education-remote-education-provision

Open data charter. (2015). *International Open Data Charter.* Available at: https://opendatacharter.net/wp-content/uploads/2015/10/opendatacharter-charter_F.pdf

Optic Humana Technologia (OPTIC). (2018). *Blockchain, Au défi de la confiance.* Available at http://optictechnology.org/images/files/Research/OPTIC2017-Blockchain-au-dfi-de-la-confiance.pdf

Pepler, G. and Andries, A. (ed). (2012). *Virtual schools and colleges: providing alternatives for successful learning. Volume 1, 119 pp.* Available at: https://lirias.kuleuven.be/retrieve/233219

Pfeffer-Gillett, A. (2018). *Peeling Back the Student Privacy Pledge, 16 Duke Law & Technology Review, pp. 100-140.* Available at: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1317&context=dltr

Plunkett, L. and Gasser, U. (2016). *Student Privacy and Ed Tech (K-12) Research Briefing.* Berkman Center Research Publication No. 2016-15. http://dx.doi.org/10.2139/ssrn.2842800

Reddy, A., Vance, A. (2020). *Social (Media) Distancing: Online Learning during a pandemic.* Available at: https://studentprivacycompass.org/social-media-distancing-covid19/

Reinsel, D., Gantz J. and Rydning J. (2017). *Data Age 2025: The Evolution of Data to Life-Critical. Don't Focus on Big Data; Focus on the Data That's Big.* IDC White Paper. Available at: https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

Roux, T. (2017). *Ces data-brokers qui font commerce de nos données personnelles.* Available at https://atelier.bnpparibas/smart-city/article/data-brokers-commerce-donnees-personnelles

Rubel, A. and Jones, K. M. L. (2014). *Student Privacy in Learning Analytics: An Information Ethics Perspective.* The Information Society, 32(2), 143-159. DOI: 10.1080/01972243.2016.1130502.

Russelll, N. C., Reidenberg, J.R., Martin, E. and Norton, T. (2018). Transparency and the Marketplace for Student Data. *Virginia Journal of Law and Technology, Forthcoming.* Available at: http://dx.doi.org/10.2139/ssrn.3191436

Salesforce. (2018). *Digital Advertising 2020. Insights into a new era of advertising and media buying.* Available at: https://www.salesforce.com/content/dam/web/en_us/www/assets/pdf/datasheets/digital-advertising-2020.pdf

Samm, S. (2018). *China's Emerging Data Privacy System and GDPR.* Available at https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr

Samm, S., Xiaomeng, L., Manyi, L. (2018). *What the Facebook scandal means in a land without Facebook: a look at China's burgeoning data protection regime.* Available at https://www.csis.org/analysis/what-facebook-scandal-means-land-without-facebook-look-chinas-burgeoning-data-protection

Sancho-Gil, J.M., Rivera-Vargas, P. and Miño-Puigcercós, R.(2020). Moving beyond the predictable failure of Ed-Tech initiatives. *Learning, Media and Technology*, 45:1, pp. 61-75. Available at: DOI: 10.1080/17439884.2019.1666873

Schwab, K. (2016). *The Fourth Industrial Revolution: What It Means and How to Respond.* Available at https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Scherer, M.U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology, 29(2).* Available at: http://dx.doi.org/10.2139/ssrn.2609777

School Education Gateway. (2018). *A brief guide to GDPR for schools and teachers*. Available at: https://www.schooleducationgateway.eu/en/pub/resources/tutorials/brief-gdpr-guide-for-schools.htm

Selwyn, N., Hillman, T., Eynon, R., Ferreira, G., Knox, J., Macgilchrist, F. and Sancho-Gil, J.M. (2020). What's next for Ed-Tech? Critical hopes and concerns for the 2020s. *Learning, Media and Technology*, 45:1, pp. 1-6. Available at: DOI: 10.1080/17439884.2020.1694945

Shah, D. (2018a). *Coursera's 2018 Revenue Estimated to be $140 million.* Available at: https://www.class-central.com/report/coursera-2018-revenue-140-million/

Shah, D. (2018b). *By the Numbers: MOOCs in 2018.* Available at: https://www.class-central.com/report/mooc-stats-2018/

Shah, D. (2019a). *By the Numbers: MOOCs in 2019*. Available at: https://www.classcentral.com/report/mooc-stats-2019/

Shah, D. (2019b). *Year of MOOC-based Degrees: A Review of MOOC Stats and Trends in 2018.* Available at: https://www.classcentral.com/report/moocs-stats-and-trends-2018/

Shah, D. (2019c). *Online Degrees Slowdown: A Review of MOOC Stats and Trends in 2019.* Available at: https://www.classcentral.com/report/moocs-stats-and-trends-2019/

Shiohira, K. and Dale-Jones, B. (2019). *Interoperable data ecosystems: An international review to inform a South African innovation.* Available at: https://www.jet.org.za/resources/interoperable-data-ecosystems.pdf

Siemens, G. and Baker, R.S.J. (2012). *Learning Analytics and Educational Data Mining: Towards Communication and Collaboration. LAK12: 29 April – 2 May 2012, Vancouver, BC, Canada.* Available at: https://dl.acm.org/doi/pdf/10.1145/2330601.2330661

Singh, P.J. (2019). *Looking Beyond Privacy: The Importance of Economic Rights to Our Data.* Available at: https://thewire.in/tech/data-privacy-digital-economy

Slade, S., Prinsloo, P., Khalil, M. (2019). *Learning analytics at the intersections of student trust, disclosure and benefit. Proceedings of the 9th International Conference on Learning Analytics & Knowledge (LAK19).* Association for Computing Machinery, New York, USA, pp. 235–244. Available at: DOI: https://doi.org/10.1145/3303772.3303796

Smolenski, N. (2016). *Identity and Digital Self-Sovereignty. A New Paradigm for Sovereignty on the High Seas*. Available at: https://medium.com/learning-machineblog/identity-and-digital-self-sovereignty-1f3faab7d9e3

State of New Mexico vs. Google LLC. Complaint. 2020. Available at: https://cdn.vox-cdn.com/uploads/chorus_asset/file/19734145/document_50_.pdf

Stringer, E., Lewin, C., and Coleman, R. (2019). *Using digital technology to improve learning: guidance report. Education Endowment Foundation.* Available at: https://educationendowmentfoundation.org.uk/evidence-summaries/evidence-reviews/digital-technology-2019/

Student Privacy Pledge. (n.d.). *K-12 School Service Provider Pledge to Safeguard Student Privacy*. Available at: https://studentprivacypledge.org/privacy-pledge/

Tang, Y. and Hew, K. (2017). Using Twitter for education: Beneficial or simply a waste of time? *Computers & Education*. 106, pp. 97-118. Available at: DOI:10.1016/j.compedu.2016.12.004

The Economist. (2018). *What the Internet of Things means for consumer privacy. A report from The Economist Intelligence Unit.* Available at: https://perspectives.eiu.com/sites/default/files/EIU_ForgeRock%20-%20What%20the%20Internet%20of%20Things%20means%20for%20consumer%20privacy.pdf

The New York Times. (2017). *How Google Took Over the Classroom*. Available at: https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html

The New York Times. (2020). *The Future of College Is Online, and It's Cheaper*. Available at: https://nyti.ms/3ejLhL2

The Washington Post. (2020). *Out of the classroom, onto the screen: Virginia teachers turn to streaming and social media*. Available at: https://www.washingtonpost.com/local/education/out-of-the-classroom-onto-the-screen-virginia-teachers-turn-to-streaming-and-social-media/2020/03/17/b70e6d2e-6872-11ea-9923-57073adce27c_story.html

U.K. Department of Education. (2014). *Cloud (educational apps) software services and the Data Protection Act. Departmental advice for local authorities, school leaders, school staff and governing bodies*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644845/Cloud-services-software-31.pdf

U.K. Department of Education. (2018). *Data protection: a toolkit for schools. Open Beta: Version 1.0.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf

UK Information Commissioner's Office. (n.d.). *Age appropriate design: a code of practice for online services.* Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

UNESCO. (2015a). *Education 2030 Incheon Declaration and Framework for Action*. Available at: http://unesdoc.unesco.org/images/0024/002456/245656e.pdf

UNESCO. (2015b). *Qingdao Declaration, 2015: Seize Digital Opportunities, Lead Education Transformation*. Available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/ED/pdf/Qingdao_Declaration.pdf

UNESCO. (2015c). *Rethinking Education: Towards a global common good?* Available at: https://unesdoc.unesco.org/ark:/48223/pf0000232555

UNESCO. (2017). *The Ljubljana Action Plan from the Second World OER Congress*. Available at: https://en.unesco.org/sites/default/files/ljubljana_oer_action_plan_2017.pdf

UNESCO. (2018a). *Digital Credentialing. Implications for the recognition of learning across borders*. Paris, UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000264428

UNESCO. (2018b). *Re-orienting Education Management Information Systems (EMIS) towards inclusive and equitable quality education and lifelong learning. Working Papers on Education Policy*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000261943

UNESCO. (2018c). *A lifeline to learning. Leveraging technology to support education for refugees*. Paris, UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000261278

UNESCO. (2019a). *Beijing Consensus on Artificial Intelligence and Education*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000368303

UNESCO. (2019b). *Preliminary study on the technical and legal aspects relating to the desirability of a standard-setting instrument on the ethics of artificial intelligence*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000367422?posInSet=2&queryId=325cbca9-7ad3-4265-8118-88c3dc451766

UNESCO. (2019c). *Anytime, anywhere learning for improved education results in Russia. Case study by the UNESCO-Fazheng project on best practices in mobile learning*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000367745

UNESCO. (2019d). *Recommendation on Open Educational Resources (OER)*. Available at: http://portal.unesco.org/en/ev.php-URL_ID=49556&URL_DO=DO_TOPIC&URL_SECTION=201.html

UNESCO. (2019e). *Mobile learning for individualized education in China. Case study by the UNESCO-Fazheng project on best practices in mobile learning*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000371930

UNESCO. (2019f). *Artificial intelligence in education: challenges and opportunities for sustainable development. Working Papers on Education Policy*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000366994

UNESCO. (2021). *Reimagining our futures together. A new social contract for education*. Available at: https://en.unesco.org/futuresofeducation/

UNESCO. (2021b). *Re-imagining the future education management information systems, beyond head counts: leveraging data systems to support inclusive and effective learning for all.* Available at: https://unesdoc.unesco.org/ark:/48223/pf0000378048

UNESCO. (2022). *Rewired Global Declaration on Connectivity for Education*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381482

UNESCO. (2022b). *UNESCO Strategy for TVET 2022-2029, Transforming Technical and Vocational Education and Training (TVET) for successful and just transitions.* Forthcoming.

UNESCO Bangkok. (2016). *A Policy Review: Building Digital Citizenship in Asia-Paci¬c through Safe, Effective and Responsible Use of ICT*. Available at: http://unesdoc.unesco.org/images/0024/002468/246813E.pdf

UNESCO and Commonwealth of Learning. (2016). Making Sense of MOOCs. *A Guide for Policy-Makers in Developing Countries*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000245122

UNESCO and Commonwealth of Learning. (2019). *Guidelines on the development of open educational resources policies*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000371129

UNESCO and EQUALS (2019). *I'd blush if I could.* Available at: https://unesdoc.unesco.org/ark:/48223/pf0000367416?1=null&queryId=8b4e3418-2bde-4f85-8d1e-c926fe7694fa

UNESCO Institute for Information Technologies in Education (IITE). (2010). *Recognizing the potential of ICT in early childhood education.* UNESCO IITE Publishing, Moscow. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000190433

UNESCO Institute for Information Technologies in Education (IITE). (2020). *Personal Data Security Technical Guide for Online Education Platforms.* UNESCO IITE Publishing, Moscow. Available at: https://iite.unesco.org/wp-content/uploads/2020/05/Personal-Data-Security-Technical-Guide-for-Online-Education-Platforms-1.pdf

UNESCO Institute for Lifelong Learning (UIL). (n.d.) *Technical Note: Lifelong Learning*. Available at: http://uil.unesco.org/fileadmin/keydocuments/LifelongLearning/en/UNESCOTechNotesLLL.pdf

UNESCO Institute for Statistics (UIS). (2018). *A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2. Information Paper No. 51.* Available at: http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf

UNICEF. (2018). *Industry toolkit: Children's online privacy and freedom of expression*. Available at: https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

United Nations, Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, (8 April 1988), available at: http://www.refworld.org/docid/453883f922.html

United Nations Human Rights Council. *Report of the Special Rapporteur on the right to privacy, Artificial intelligence and privacy, and children's privacy*, (25 January 2021), A/HRC/46/37, Available at: https://undocs.org/A/HRC/46/37

United Nations Human Rights Council, *Report of the Special Rapporteur on the right to privacy, Right to privacy*, (16 October 2019), UN. Doc 1/HRC/40/63, Available at: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session40/Pages/ListReports.aspx

United Nations, Human Rights Council, *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, (18 June 2018), UN. Doc A/HRC/38/47, Available at: https://digitallibrary.un.org/record/1641160

United Nations, General Assembly, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Martin Scheinin, A/HRC/13/37 (28 December 2009), Available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/a-hrc-13-37.pdf

United Nations, General Assembly, *Impact of rapid technological change on the achievement of the Sustainable Development Goals and targets,* A/75/316 (19 August 2021), Available at: https://undocs.org/pdf?symbol=en/A/RES/75/316

United Nations Development Group (UNDG). (2017). *Data privacy, ethics and protection: guidance note on big data for* *achievement of the 2030 agenda*. Available at: https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda

United States, Federal Trade Commission. (2014). *Data Brokers. A Call for Transparency and Accountability.* Available at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

United States. State of California. (2016). *California Student Online Personal Information Protection Act*. Available at: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177

U.S. Department of Education, Privacy Technical Assistance Center (PTAC). (2014). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. Available at: https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best

U.S. Department of Education, Privacy Technical Assistance Center (PTAC). (2017). *Integrated Data Systems and Student Privacy.* Available at: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/IDS-Final_0.pdf

Van Den Beemt, A., Thurlings, M. and Willems, M. (2020). Towards an understanding of social media use in the classroom: a literature review. *Technology, Pedagogy and Education*, 29:1, pp. 35-55. Available at: DOI: 10.1080/1475939X.2019.1695657

Villani, C. (2018). *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*. Available at: https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf

Waldman, A.E. (2018). *Privacy as trust: information privacy for an information age*. New York, Cambridge University Press.

Wood, C. (2020). *Indiana University accidentally shares grades of 100,000 students*. Available at: https://edscoop.com/indiana-university-accidentally-shares-grades-100000-students/

World Economic Forum (WEF). (2011). *Personal Data: The Emergence of a New Asset Class*. Available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

World Economic Forum (WEF). (2015). *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*. Available at: http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

World Economic Forum (WEF). (2016). *6 ways social media is changing the world*. Available at: https://www.weforum.org/agenda/2016/04/6-ways-social-media-is-changing-the-world/

World Economic Forum (WEF). (2017). *Realizing the Potential of Blockchain. A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies*. Available at https://www.weforum.org/whitepapers/realizing-the-potential-of-blockchain

World Economic Forum (WEF). (2018a). *Digital Identity, On the Threshold of a Digital Identity Revolution*. Available at http://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf

World Economic Forum (WEF). (2018b). *Our Shared Digital Future. Building an Inclusive, Trustworthy and Sustainable Digital Society.* Available at: http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf

World Economic Forum (WEF). (2019a). Over 2.5 billion people use social media. *This is how it has changed the world*. Available at: https://www.weforum.org/agenda/2019/10/rise-of-social-media

World Economic Forum (WEF). (2019b). *Data Collaboration for the Common Good. Enabling Trust and Innovation Through Public-Private Partnerships.* Available at: http://www3.weforum.org/docs/WEF_Data_Collaboration_for_the_Common_Good.pdf

World Economic Forum (WEF). (2019c). *Our Shared Digital Future. Responsible Digital Transformation*. Board Briefing. Available at: http://www3.weforum.org/docs/WEF_Responsible_Digital_Transformation.pdf

World Economic Forum (WEF). (2019d). *Outbreak Readiness and Business Impact Protecting Lives and Livelihoods across the Global Economy*. White Paper, in collaboration with Harvard Global Health Institute. Available at: https://www.weforum.org/whitepapers/outbreak-readiness-and-business-impact-protecting-lives-and-livelihoods-across-the-global-economy

World Economic Forum (WEF). (2020). *The global risks report 2020*. Available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

WIPO. (2019). *WIPO Technology Trends 2019: Artificial Intelligence*. Geneva: World Intellectual Property Organization. Available at https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

Witte, J. (2016). *The Blockchain: A Gentle Introduction*. Available at https://ssrn.com/abstract=2887567

World Bank. (2020). *Guidance Note on Remote Learning and COVID-19* (English). Washington, D.C. World Bank Group. http://documents.worldbank.org/curated/en/531681585957264427/Guidance-Note-on-Remote-Learning-and-COVID-19

World Bank. (2020). *Remote Learning, Distance Education and Online Learning During the COVID19 Pandemic: A Resource List by the World Bank's Edtech Team* (English). Washington, D.C. World Bank Group. http://documents.worldbank.org/curated/en/964121585254860581/Remote-Learning-Distance-Education-and-Online-Learning-During-the-COVID19-Pandemic-A-Resource-List-by-the-World-Banks-Edtech-Team

World Wide Web Foundation. (2015). *Women's Rights Online: Translating Access into Empowerment*. Geneva, Web Foundation, Available at: https://webfoundation.org/research/womens-rights-online-2015/

Wunderlich, J. (2020). Post-Pandemic Privacy Preservation. *LinkedIn* Article Post. https://www.linkedin.com/pulse/post-pandemic-privacy-preservation-john-wunderlich/

Zeide, E. (2017). The Structural Consequences of *Big Data*-Driven Education. Big Data, 5(2), pp. 164-172. Available at SSRN: https://ssrn.com/abstract=2991794

Zeide, E. (2018). Education Technology and Student Privacy. In E. Selinger, J. Polonetsky, and O. Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, pp. 70–84. Cambridge, Cambridge University Press. Available at SSRN: https://ssrn.com/abstract=3145634

unesco
United Nations
Educational, Scientific
and Cultural Organization

Minding the data

Protecting learners' privacy and security

The COVID-19 pandemic and the migration of education systems to remote and digital learning has accelerated the use of digital technologies in education. In addition to the emergency response, there is an international trend to explore how AI and data-based analytics can support learning, learning assessments and evidence-based policy planning processes. This trend has two effects. The first is the need for large data sets drawn from aggregation of learning profiles, micro-behaviours, access time and online actions, to build patterns and better understand learning processes, effectiveness and problems. The second is a change in approach to the concept of privacy and security.

There is a broad agreement that proper rules and protocols are needed to protect students and teachers from overreach. While national policies and regulations are needed, international cooperation and collaborative efforts are also required to support policy learning, knowledge sharing and mutual understanding. The continued reinforcement of learners' data protection and security will require actions to build shared knowledge, norms and standards. While not completely silent on matters of data privacy, ongoing international processes are certainly in need of strengthening.

This publication explores early responses from the education sector to the question of managing data privacy in this era of accelerated digitization, even further accelerated by the COVID-19 pandemic. It serves as a clarion call to the sector not only to pay careful attention to data privacy in education, but to take the lead in these developments. Learner data are particularly vulnerable to data breaches in a more digitized world, while those same technologies provide the opportunity for more futuristic notions of 'credentialling' that transcend the formal, non-formal and informal divides that have long impeded our ability to realize the full potential of lifelong learning.

9 789231 005251

4 QUALITY EDUCATION

Sustainable Development Goals