4 Guidance and regulatory frameworks for digital education

This chapter reviews the current guidance and regulations in place across OECD countries with respect to digital education. It highlights the nascent nature of many aspects of regulatory frameworks from the viewpoint of protecting learners in digital environments and ensuring their equitable access to the benefits of digital education. The chapter also stresses the need to ensure that quality assurance policies and practices are adapted and, where necessary, updated to take specific considerations related to digital education into account. Regulatory frameworks should also be designed to ensure compliance with important legal and ethical requirements related to digitalisation, such as child protection, data protection and the impact of AI and algorithms.

Introduction

This chapter examines the elements of a fit-for-purpose guidance and regulatory framework that can promote effective digital education and adapt to evolving needs, while protecting and supporting learners. Digital transformation of education requires ongoing policy efforts to provide and update guidance, standards and regulations. Accounting for specific education governance arrangements and understanding the distribution of roles and responsibilities in the education systems for digital education is crucial for this purpose. A fit-for-purpose policy framework for digital education is also one that leverages the involvement of all digital education stakeholders and ensures they can meaningfully contribute to seizing the potential of digital technologies in education systems.

Increasing cyber security risks, concerns about data protection and potential algorithmic bias increase the need for closer attention to the design of new guidance for compliance with existing digital security and data protection frameworks, and for regulation in areas that currently remain largely uncovered. This chapter examines the provision of standards, guidelines and formal regulations (with an associated legal obligation) to enable an efficient and safe use of digital education technologies. Public bodies need to provide support and guidance to education institutions for many aspects of digital education. These include compliance with legal and regulatory frameworks, making investment decisions, maximising technology interoperability and ensuring privacy protection and equitable practice.

Quality standards and guidelines for digital education can support institutions in making effective use of digital technologies that translate into better student outcomes. This requires developing a coherent quality assurance approach for digital education, clarifying focus areas to be covered as well as the intended use of the evaluation results (for accountability, identifying and promoting good practices and improving provision where it does not meet the required standards). There is also a need to ensure synergies and articulations between processes and tools to ensure coherence and consistency. International co-operation and co-ordination on setting standards for digital education technologies can support quality assurance efforts.

Education systems face a range of challenges in providing adequate governance and regulatory frameworks for digital education. This chapter aims to address these challenges by taking stock of the relevant evidence and presenting some promising policy examples from OECD and EU countries. Some of the key questions on this issue that policy makers need to consider include:

- How can education systems build a regulatory framework, design guidance and institutional capabilities that enable the protection of learners and ensure the quality of digital education?
- How can the regulatory framework for digital education be designed to adequately steer the use of emerging or fast-evolving technologies?
- How can education systems address the governance implications of increasingly digitalised schools and growing reliance on hybrid learning?
- How can education systems best engage different stakeholders to help achieve the potential of digital technologies in education?

Recent developments and current challenges

Learner protection measures and equitable practices in digital learning environments remain insufficient

Learners can face a wide variety of risks in a digital learning environment

Whilst digital technologies bring a wealth of opportunities to enhance learning experiences, they also entail a set of risks for learners and teachers. Responses from 34 countries to a 2017 OECD Policy Questionnaire on the protection of children online revealed a wide variety of online risks faced by children and considered to be relevant by policy makers (e.g. bullying, online privacy, hateful content, harmful overuse of connected devices and online services) (OECD, 2020[1]). Beyond potentially affecting children's development and well-being, these risks might also have tangible effects on their rights (e.g. right to privacy, right to no discrimination).

Students are also likely to face these risks when using digital technologies for learning. As the use of digital technologies in learning processes has expanded significantly throughout the pandemic, the risks entailed by digital technologies increasingly permeate education systems. For instance, the COVID-19 pandemic has substantially increased the amount of data shared in education settings, translating into heightened privacy risks for students (OECD, 2021[2]).

Education software or digital education platforms that reach students through schools may be subject to tight data protection or privacy regulations that may help mitigate against risks, especially if their developers follow principles of safety by design (UNICEF, 2022[3]). At the same time, such built in protections may not always be sufficient. Students may, for instance, still be vulnerable to cyberbullying through e-learning platforms or be exposed to a variety of risks (e.g. harmful content) when looking for information online for schoolwork. The collection, use and reuse of children's data from such platforms may also be problematic for children's privacy (OECD, 2022[4]). In addition, children may also be exposed if they disclose personal information unintentionally during learning processes, share or upload inappropriate content, or infringe on copyrights or other rights through plagiarism (UNICEF, 2022[3]).

This wide variety of risks that children potentially face in a digital learning environment increases the need for a co-ordinated and comprehensive legal and policy response. Almost all countries responding to the OECD Policy Questionnaire on the protection of children online in 2017 had introduced some form of legislative or policy response to address the risks faced by children in a digital learning environment (OECD, 2020[1]; Burns and Gottschalk, 2019[5]). At the time of the survey, however, most countries displayed fragmented approaches to children's protection in digital environments. Since then, the introduction of the General Data Protection Regulation (GDPR) in EU countries has translated into a heightened recognition of the special attention and protection children need with respect to their personal data, as well as increased efforts to raise public awareness regarding the processing of children's personal data (OECD, 2020[1]).

Enforcement likely varies across education institutions falling under European data protection regulations

The demand to show compliance in information security has been growing in the education sector, in line with the implementation of stricter regulation of the digital sphere, including the GDPR in Europe (EUR-Lex, 2016[6]). The GDPR considerably raised the level of accountability for European education institutions on the data they possess and collect, including data handled by third parties. To ensure GDPR compliance, education institutions need to:

- ensure all staff are informed about GDPR and understand how data is collected and stored and the implications of a breach (e.g. through training), including the need to report any instance to the Information Commissioner's Office (ICO);
- have systems in place to gather parental consent for data processing and verify individuals' ages;
- centralise information on software used for teaching and data collection as well as ensuring that all software comply with the GDPR;
- employ or assign a Data Protection Officer with a comprehensive knowledge of new data protection law to liaise with the ICO.

While the mandatory nature of GDPR standards promotes progress on data protection in education institutions, enforcement of the GDPR has likely varied across EU countries due to differences in the human, financial and technical resources devoted to enforcement (Ruohonen and Hjerppe, 2022[7]). In the higher education sector, survey data for 2020 indicated that 25 out of 43 NRENs in the Géant network stated having a privacy notice (including adherence to the GDPR) and 11 stated otherwise, indicating that by 2020 progress on GDPR compliance was not yet complete (Géant, 2020[8]).

While estimates on enforcement fines remain inaccurate since not all fines are made public, evidence suggests that data protection agencies had fined more than 20 education institutions (schools and universities) by 2022 across the EU. Fines were granted for a range of GDPR violations (mostly due to insufficient legal basis for data processing and insufficient technical and organisational measures to ensure information security) (CMS, n.d.[9]). The legal framework and consequences of non-compliance increase the pressure on education institutions to invest in data protection measures.

Applications of Artificial Intelligence in education require further research and regulatory efforts to protect learners and their rights

Applications of AI in education can raise concerns for learners' rights, such as their right not to suffer from discrimination, as well as for principles such as the transparency and explainability of AI systems, which are anchored in documents such as the UNCRC or national data protection laws (Holmes et al., 2022[10]). These concerns are particularly acute in situations where AI-based tools are used for high-stake decisions in education settings and without human oversight. Evidence on AI-powered education technologies, including early warning systems or classroom analytics, shows challenges related to algorithm accuracy (OECD, 2021[11]). In addition, many concerns remain about the potential bias of algorithms which can penalise specific population groups. Research highlights the manifestation of algorithmic bias in education with respect to a number of demographic categories (gender, ethnicity and nationality) (Baker and Hawn, 2021[12]). Furthermore, since research has tended to focus only on a selected number of demographic groups, it is likely that biases experienced by other demographic groups remain unidentified and undocumented, calling for further work to enhance the accuracy of algorithms.

High-stakes decisions in education systems made on the basis of potentially inaccurate or biased algorithms may lead to equity issues and unfairness in students' opportunities and outcomes. Even beyond algorithmic bias, the use of AI might have adverse effects on children's rights – including their rights to human dignity or autonomy – by diminishing the transparency and blurring the accountability of high-stakes decisions such as grading or grade-repetition (Holmes et al., 2022[10]). However, the risks and benefits of using advanced technologies must be assessed not only in absolute terms, but also relative to current arrangements. There is substantive evidence to suggest that teachers' implicit biases can impact high-stakes decisions in education systems (Bonefeld and Dickhäuser, 2018[13]). Whilst outsourcing such decisions to advanced technologies does not necessarily combat these biases, AI systems that are built with an equity lens can have the potential to detect and help teachers correct for existing biases (Perry and Turner-Lee, 2019[14]).

Regulatory efforts are thus needed to ensure that AI applications and their use in education settings are compliant with students' rights and a driving force against bias and discrimination in education systems. However, most OECD countries currently lack regulations for algorithms (OECD, 2021[11]), although a number of countries are considering regulations to enhance the transparency and accuracy of automated decision-making systems (Casovan and Shankar, 2022[15]). While the provisions on algorithm use in the GDPR are subject to conflicting legal interpretations and thus provide only limited guidance (OECD, 2021[11]), more recent efforts seek to design legislation targeting AI use in high-risk fields.

Education systems face increasing pressure to improve digital security and design digital risk-management approaches

Cyber security is the practice of protecting systems, networks and software programmes from digital attacks. The importance of cyber security has risen in recent years, given the reported significant and rising incidence of cyber-attacks, including phishing, ransomware and distributed denial of service attacks, as well as growing geopolitical tensions with risks of associated cyber-attacks. Education institutions are not immune to such cyber-attacks. Cyber security risks have rapidly expanded in education systems, in part due to a growing reliance on mobile devices, an expansion of remote or hybrid learning, and an increase in third-party education partners, which create more login points and a proliferation of vulnerable login credentials. Learners are also using education institution accounts to log in to a wider range of services: administrative portals, remote video and learning tools, and student web applications. This expansion of risk points drives an increase in data breaches and a surge in threats targeting vulnerable digital systems.

The security portfolio of education institutions to help mitigate attacks and vulnerability has grown in tandem with the rise in security risks. In larger education institutions it includes not only requirements for up-to-date operating systems and software and anti-virus software, but also more sophisticated tools such as Multi Factor Authentication, Virtual Private Networks (VPNs), end-user device management and remote data deletion.

In higher education, most NRENs in Europe have some kind of security audit of their organisation (Géant, 2020[8]). NRENs increasingly play a role in cyber security through network monitoring, specialist support when an institution comes under attack, and providing vital notifications of emerging threats and associated recommended actions. In some education systems cyber security services are provided by private firms that provide managed security services. These firms act to mobilise attention to cyber security risks – and offer commercial solutions to the risks they identify.

Progress in the implementation of interoperability frameworks has been slow in education systems

Interoperability is the ability of two or more systems (or components) to exchange information and use it in a seamless way, regardless of who the provider of the system is. Interoperability matters for access, quality, efficiency and security: it lowers the costs of technological transition, makes systems more adaptable by lowering the risk of provider lock-in, and allows for better monitoring of data and systems.

Education data and systems operate within general interoperability frameworks, including the European Interoperability Framework (European Commission, 2022[16]) and national frameworks where they exist, which are in some cases made specific to the education sector (e.g. the *Référentiel général d'interopérabilité* in **France** (République Française, 2020[17]) with more general technical guidelines including interoperability aspects currently under development). Institutions may complement these broader frameworks with one of the multiple public and proprietary interoperability standards and frameworks for education. However, progress in the implementation of interoperability frameworks has been slower in education, particularly compared to other sectors such as healthcare. Interoperability among learning environments remains insufficiently developed, triggering challenges with respect to the sustainability and affordability of digital education technologies (OECD, 2021[11]).

Quality assurance frameworks are not yet fully adapted to digital education

Evaluation and assessment tools are not always tailored to digital education

In school education systems, quality assurance policies and practices have become increasingly varied, including school self-evaluations, external school evaluations, national examinations, teachers and school leader appraisal, etc. The progressive increase in school autonomy has been associated with rising responsibilities for schools in the area of quality assurance (e.g. through a focus on school self-evaluations).

At the school level, internal and external evaluation mechanisms can play a role in enhancing the use of digital technologies for learning, teaching and management, although more needs to be done in adapting such mechanisms for digital education. Prior to the pandemic in 2018/19, 10 EU countries had included aspects related to digital education in their external school evaluation frameworks, with varying evaluation methods and data sources (e.g. surveys, classroom observation) (European Commission/EACEA/Eurydice, 2019[18]).

In **Estonia**, broader surveys on well-being at school include questions targeted to students, parents and teachers on the use of digital devices for learning, guidance received by students from teachers in this area, etc. In addition, students' digital competence was assessed as part of quality assurance procedures in lower and upper secondary education (European Commission/EACEA/Eurydice, 2019[18]). Schools were equally in charge of self-reporting on their digital infrastructure for education. In contrast, in other countries, such as **Romania** and **Latvia**, external school evaluation frameworks only focused on the availability of digital infrastructure for education, which likely limited their ability to assess the outcomes of learning with digital technologies. In a few other countries, the use of digital technologies for management purposes was also examined as part of external school evaluations.

More attention is needed regarding the design and scope of evaluation frameworks and tools, in order to adapt them to collect useful information about digitalisation. Relevant topics to be covered may include the quality of digital infrastructure, and teachers' and school leaders' preparedness to work with digital technologies. More consideration could also be given to the ways of using the results of such evaluations (e.g. for identifying and promoting good practices).

More recent developments of digital education strategies, as well as pandemic-related measures for digital education, suggest that countries are increasingly putting an emphasis on quality assurance tools for digital education. The rise in the provision of online school education has also triggered increased demand for regulation of online learning provision in some countries. For instance, in the **United Kingdom**, the Department for Education is developing an Online Education Accreditation Scheme targeted at providers of full-time online education for children who cannot attend school in person (GOV.UK, 2021[19]). The new accreditation aims at increasing standards of full-time online education, while also informing parents' choices. The scheme relies on establishing non-statutory standards for online education provision and inspection of providers against these standards by the Office for Standards in Education, Children's Services and Skills (a non-ministerial department in charge of inspecting education providers for all ages and skills).

Beyond quality assurance for online learning, the pandemic has also triggered an increase in policy efforts aimed at expanding the provision of digital education resources more generally but also at better assessing and certifying their quality. Systematic and comprehensive cross-country evidence on how countries have adapted and developed their quality assurance strategies for digital school education remains, however, relatively limited.

Some transnational quality assurance organisations have developed specific guidance for the quality assurance of e-learning in higher education

In European higher education, the European Network for Quality Assurance Agencies in the European Higher Education Area (ENQA) seeks to encourage quality assurance agencies and HEIs to use the *European Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG)* (E4 Group, 2015[20]). The ESG provide a set of standards and guidelines[1] for internal and external quality assurance related to “learning and teaching in higher education, including the learning environment and relevant links to research and innovation”. The ESG (2015[20]) state that the standards and guidelines apply to “all higher education offered in the EHEA regardless of the mode of study or place of delivery” (E4 Group, 2015[20]), an approach seconded by other international quality assurance networks. For instance, in its *Guidelines of Good Practice*, the International Network of Quality Assurance Agencies in Higher Education (INQAAHE) states that their “standards or criteria take into consideration the specific aspects related to different modes of provision, such as transnational education, distance or online programmes or other non-traditional approaches.” (INQAAHE, 2018, p. 7[21]).

While INQAAHE and ENQA do not believe it is necessary to revise the overarching approach to quality standards, they have suggested that quality assurance agencies and HEIs include specific e-learning considerations in their existing quality frameworks, adapt existing evaluation methods and strengthen their internal expertise for the evaluation and revision of digital study programmes. To support the development of specific quality standards for digital higher education, an ENQA Working Group has developed “Considerations for the quality assurance of e-learning provision” (Huertas et al., 2018[22]). The report includes a list of “elements to consider” and “indicators”, but they are not legally binding for quality assurance agencies and institutions and have been developed independently from the ESG. In addition, INQAAHE’s 2022 release of international standards and guidelines for quality assurance includes a specific module on online and blended modalities (INQAAHE, 2022[23]).

Few national quality assurance agencies have developed standards and processes for the quality assurance of digital higher education

Many national higher education quality assurance agencies in Europe have not yet developed quality standards and processes to degree programmes in fully online or hybrid formats. They have found it challenging to develop a shared understanding of what quality in digital higher education means (Tait, 2022[24]; Gaebel et al., 2021[25]) and to adapt standards and processes developed for traditional face-to-face provision to digital provision. Many quality assurance agencies lack institutional capacity or expertise to expand the scope of their activities to encompass digital provision. This is particularly relevant in smaller EU jurisdictions and for quality assurance agencies that carry heavy administrative responsibilities arising from their role as accreditors of individual study programmes.

Programme accreditation processes can also support or inhibit the expansion of digital study programmes offered by higher education institutions. For example, in **Hungary** there were only 45 accredited fully online distance learning (DL) programmes on offer in 2021, which represents a small share of the total of 11 246 accredited higher education study programmes in the country (FELVI, 2021[26]). One reason for this is that higher education institutions must meet a number of detailed “special provisions for distance education programmes” (Netjogtar, 2022[27]) in addition to a core set of requirements applicable to all programmes regardless of their delivery mode. Similarly, in **Croatia**, online programmes must meet a strict set of specific criteria in order to be accredited by the quality assurance agency (OECD, 2023[28])

To encourage institutions to offer more high-quality DL programmes, **Romania** recently revised its *ex-ante* programme accreditation procedures, providing institutions with the opportunity to be granted “provisional operation authorisation” for DL programmes if they have the required financial and online learning resources in place to offer at least one full study cycle. Within two years of launching the DL programme, institutions need to apply for full programme accreditation (ARACIS, 2020[29]).

Many European HEIs already have internal quality standards in place for digital education

The primary responsibility for quality assurance lies with HEIs themselves. A major survey of 368 institutions from 48 European countries administered in 2020 by the European University Association (Gaebel et al., 2021[25]) found that 51% of HEIs had already integrated digitally enhanced teaching and learning considerations in their internal quality assurance procedures, and measures were under development in another 41% of responding institutions. This represents a significant increase compared to 2014, when the figures were 29% and 35% respectively. This shift is driven by the priority attached to digitalisation: three-quarters of survey respondents had concrete plans to boost digital capacity beyond the pandemic, and 95% saw digitalisation as a strategic priority over the next five years.

Promising approaches for creating an effective guidance and regulatory framework

Establish a regulatory framework to guide digital education, and ensure it is adaptable to evolving needs

Provide guidance and resources to support compliance with existing digital security and data protection frameworks

Education institutions across OECD countries face increasing challenges in ensuring the security of their activities online and complying with regulations aimed at supporting the privacy of their learners' data. While the regulatory framework might be present, compliance with its requirements often requires additional resources. In this context, some countries provide guidance for education institutions, teachers and learners, as well as practical and content related resources to help them adapt in a fast-changing technological and regulatory environment:

- In **France,** the Ministry of Education and the national data protection authority signed an agreement in 2015 to provide training and resources for raising awareness and preparing teachers and school leaders on GDPR processes (OECD, 2020[1]). In addition, the national data protection authority developed a reference framework for the training of students specifically devoted to data protection (Eduscol, 2022[30]). The framework is intended to be used as part of school courses as well as in the training courses of education staff, regardless of the subject taught, with the aim of building a common base of concrete skills in the field of personal data protection. Initiated by the French national data protection authority, the reference framework was also adopted at the international level by other data protection authorities in 2016 (International Working Group on Digital Education, 2016[31]). Beyond building capacity and providing guidance on data protection, the French Ministry has also provided practical resources to secure user data. For instance, the GAR (*Gestionnaire d'Accès aux ressources*) is an authentication system supported by the French Ministry of Education that allows students and teachers to access education material through a single identifier, thus enhancing security and protecting users' personal data (Ministère de l'éducation nationale, n.d.[32]).
- The Department for Education in the **United Kingdom** prepared a data protection toolkit to support schools with data protection activities and compliance with the Data Protection Act that implements the GDPR (Department for Education, 2019[33]). In addition, the National Cyber Security Centre provides practical resources targeted at school governing boards, senior leaders and school staff to support their understanding of cyber security, help them work safely on line, and effectively detect, manage and solve any incidents (NCSC, 2021[34]).
- The **United States** Department of Education has created a Privacy Technical Assistance Center (PTAC) which provides privacy toolkits and training materials for the benefit of education institutions at early childhood education and care, school and post-secondary levels, as well as for

the benefits of parents and students. It is designed to be a "one-stop" resource for queries related to privacy and data protection in education (US Department of Education, n.d.[35]).

Design a co-ordinated policy approach to support children's protection in digital learning environments

As described previously, students' uses of digital tools for education purposes are not contained to designated learning platforms. Rather, students draw on a range of online resources when searching for learning-related information. Many countries have thus taken a holistic approach to address risks stemming from children's engagement in digital environments (e.g. cyberbullying, data privacy-related risks, harmful content) including but not limited to digital education environments. Regulations have targeted the providers of digital technologies, services or content and – in the context of digital education – those involved in the use of such technologies for learning (e.g. education institutions, teachers). As part of the OECD Recommendation of the Council on Children in the Digital Environment, the OECD has put forward guidelines for digital services providers calling on them to adopt a "child safety by design" approach, ensure effective information provision transparency and accountability, establish safeguards and take precautions regarding children's privacy and data protection (OECD, 2021[36]).

Other efforts for international co-operation or co-ordination regarding standards-setting on children's data protection have also emerged. For instance, the International Conference of Data Protection and Privacy Commissioners' working group on digital education has passed resolutions on e-learning platforms and privacy in education (OECD, 2020[1]). At the national level, as of 2017, co-ordinated and targeted approaches for the protection of children in digital environments were not widespread yet, although a few OECD countries had accompanied more targeted legislation with the establishment of statutory oversight bodies for online privacy protection (OECD, 2020[1]).

Further co-operation at the national level should accompany international co-operation efforts on children's protection in digital learning environments. Education authorities should be engaged in regulatory efforts or discussions at the government level to ensure specific risks related to the use of digital technologies in education are taken into consideration in the design of legal or policy responses. Designing an appropriate legal and regulatory framework to guide a safe use of digital technologies in learning processes also requires co-operation among a variety of stakeholders for child protection. Such stakeholders may include education institutions, teacher and parent organisations, digital education technology developers and the research community, as well as government authorities and agencies with responsibilities for education, child protection, and social services. (UNICEF, 2022[3]).

Share services to achieve standardisation and cost-efficiency in data protection and cyber security solutions

Considering the growing significance and complexity of data standards, prior OECD recommendations advocate for appointing national expert panels to evaluate, compare, and enhance government and institutional digital and data policies, encompassing personal data protection, content sharing and usage, and data integrity within digital learning environments (OECD, 2021[37]).

Networks and associations can provide an effective vehicle to promote compliance with data protection frameworks in education institutions:

- In **Europe**, Géant provides training and support documents on data protection compliance to its member organisations. It also hosts a special interest group on information security management where Chief Information Security Officers exchange knowledge and experiences. A task force of security incident response teams also works to improve co-operation and co-ordination, to promote the use of common standards and procedures for handling security incidents, and to co-ordinate joint initiatives, including training for security staff (Géant, 2020[8]).

- In **the Netherlands**, SIVON (a co-operative of school boards) together with SURF entered an agreement with Google on behalf of education institutions to ensure that Google does not use data collected through Google services and Chromebooks from schools and students for its own purposes (SIVON, 2022[38]).

In addition, such networks, associations and co-operatives have also emerged as providers of security services for education institutions:

- In **Australia**, AARNet (Australian Academic and Research Network) provides connectivity and security services to K-12 schools and research communities across the country (AARNet, n.d.[39]). Services offered include education roaming, private cloud connections or virtual private networks. AARNet is run by a not-for-profit company that is owned by Australian Universities and the government's research agency (AARNet, n.d.[40]).
- In **Europe,** NRENs increasingly play a role in cyber security through network monitoring, specialist support when an institution comes under attack, and providing a vital source of advice and notification, both on emerging threats and immediate actions. In fact, most NRENs in Europe have some kind of security audit of their organisation (Géant, 2020[8]). Given the considerable investment needed, only the largest NRENs in Europe have started moving their security services to security operations centres. Moreover, Géant offer shared security services to NRENs including a Trusted Certificate Service (used by 33 NRENs in 2020), a Firewall on Demand (used by 28 NRENs) and eduVPN a state of the art, privacy-preserving VPN service (Géant, 2020[8]).

Support the development of policies, standards, or guidelines for monitoring algorithm and AI use and impact in education

Regulations surrounding the use of algorithms and AI in education are not yet widespread in OECD and EU countries, although there are emerging efforts to regulate their use more broadly (e.g. the Algorithmic Accountability Act of 2022 proposed in the **United States**). Education is a critical area of application for AI and algorithm-based tools, with a 36% estimated growth expected in the size of the education AI market between 2022 and 2030 (Grand View Research, 2021[41]). Against the background of growing concerns on the impact of algorithm bias in education, the increasing uptake of these new technologies must be matched by new regulatory efforts.

Some efforts have already been made to set guidelines for AI in more general terms, such as the OECD AI principles described in Box 4.1. While the development of general regulations for AI and algorithm-based tools has a wider scope than the education sector, education sector stakeholders and experts must be engaged in the development of these legislations to ensure the specific needs of the education sector are met (Baker and Hawn, 2021[12]; Turner Lee, Resnick and Barton, 2019[42]; OECD, 2021[11]). Further efforts to support research on algorithmic bias in education are also needed, including support for improvements in data collections (particularly on underrepresented demographic groups in current research), additional funding for research and for designing education-specific tools to conduct bias audits (Baker and Hawn, 2021[12]).

Beyond participating in government-level regulation of the use of AI and algorithm-based tools, educators must be further empowered to use these education technologies responsibility and carefully and to critically question their implications on privacy and fairness. This requires formulating and disseminating guidelines for the application of AI and algorithm-based tools in education. There are first indications for efforts in this field, both on an international and national level:

- In **Europe**, the European Commission has recently provided ethical guidelines on the use of AI and data in teaching and learning (European Commission, 2022[43]). The guidelines aim to inform educators about the potential of AI applications for education and raise awareness of possible risks.

- In March 2023, the Department of Education in the **United Kingdom** released a policy position paper on the use of generative AI in education systems, highlighting the responsibilities of schools, colleges, universities and awarding institutions to avoid malpractice using the technology and to continue to ensure that data is protected (Department for Education, 2023[44]). At the same time, the paper highlights the potential for generative AI to reduce workload across the education sector, and free up staff time to focus on delivering excellence in teaching.

Box 4.1. OECD AI principles

The OECD AI principles set international standards for innovative and trustworthy AI which respects human rights and democratic values. Since their adoption as part of the OECD Council Recommendation on Artificial Intelligence in 2019, all OECD member countries as well as Argentina, Brazil, Egypt, Malta, Peru, Romania, Singapore and Ukraine have signalled their political commitment to the following principles:

- AI should drive inclusive growth, sustainable development and well-being.
- AI systems should be designed to respect the rule of law, human rights, democratic values and diversity and should include appropriate safeguards towards this end.
- There should be transparency and responsible disclosure around AI systems.
- AI systems must function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed.
- Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.

Consistent with these value-based principles, the OECD also provides recommendations to governments related to facilitating investments into R&D in AI, creating an adequate policy environment for trustworthy AI systems or ensuring equitable access to AI ecosystems. Whilst the OECD AI principles are not limited to the education sector, they provide an example of internationally agreed standards that countries might want to adhere to when designing education-specific guidance and regulation for the use of AI.

Source: OECD (2019[45]), *The OECD Artificial Intelligence (AI) Principles - OECD.AI*, https://oecd.ai/en/ai-principles (accessed on 31 May 2023).

Develop policies that support interoperability of technologies and portability of data

A lack of interoperability of digital technologies used in schools and higher education institutions creates administrative and operational inefficiency, elevates the risk of vendor lock-in and hampers capacity to develop performance and learning analytics. Governments may act on a number of fronts to support interoperability of digital technologies within and across individual institutions and education systems.

Interoperability can be improved through greater use of open standards for digital education technologies. Governments and education stakeholders have a role to play in both developing and encouraging the adoption of open standards. For maximum efficiency and utility, and to increase the likelihood of their widespread adoption, standards may be most usefully established at international level, through collaborative networks of national education stakeholders and experts. In **Europe**, examples of notable initiatives to develop open standards for education technologies include the standards developed by 1Edtech (formerly IMS Europe, a subgroup of IMS Global Learning Consortium) which cover learning platforms, learning data and analytics, integrated assessment tools and standards (1Edtech, n.d.[46]) and the standards of the Europass Digital Credentials Infrastructure for issuing and sharing evidence of learning undertaken in European education systems (European Union, n.d.[47]).

Education institutions and educators may also require support to ensure the interoperability of various tools. Given that education institutions in some systems have already widely adopted LMS (Brown, Millichap and Dehoney, 2015[48]), ensuring that new technological tools can be integrated into the most widely used LMS can help to make them available to educators in a cost-effective manner and at scale.

Governments can also inform and encourage education institutions to commit to open standards and embed interoperability as a core criterion when adding to or upgrading their individual technology stacks. For example, procedures for school inspections and quality assurance evaluations of HEIs could include reflection on the extent to which technologies in use are interoperable and aligned with open standards. Governments can also facilitate knowledge-sharing about the importance of open technologies, and support platforms for institutions to share strategies and practices that successfully break down data silos and enhance interoperability. Finally, public authorities can explore ways to standardise the technologies in use across institutions as much as possible, to minimise interoperability challenges – for example by supporting large-scale procurements of technologies, or by directly providing or encouraging the use of software that adheres to open standards.

Interoperability frameworks have already been designed and developed in some education systems, as a means to improve the effectiveness and efficiency of digital education technologies. Examples include:

- The National Schools Interoperability Program (NSIP) in **Australia** promotes common technical standards and supports aiming to improve the interoperability of information systems used by schools and school authorities across Australia. A Steering Group comprising national, state and territorial education authorities oversees the work, and a small group of professionals work continuously on the project, engaging schools, standard-setting bodies and EdTech firms. It supports the widespread adoption of the Systems Interoperability Framework (SIF), an open standard used to link individual data systems in the school sector. The SIF has also been widely adopted in the UK and the USA (NSIP, n.d.[49]).
- In **Germany**, the Federal Ministry of Education and Research is funding the development of a digital education platform or hub to integrate education platforms at the national level. A network of university, civil society and business stakeholders is supporting the project that builds on previous experiences with interoperable solutions in the higher education sector. One of the prototypes developed as part of the project will enable testing structures for data exchange and interoperability of different platform types, while accounting for the federal structure of the German education system (BMBF, 2021[50]).
- In **Portugal**, the “IES+ Perto” project brought together four Portuguese higher education institutions, in collaboration with the Portuguese NREN and the Portuguese National Security Office to develop a range of technologies to improve interoperability, including a common cloud infrastructure (cloud4IES) and an interoperability platform (PI4IES) that standardises communications with the diverse administration systems in each institution, allowing for seamless transfer of students between institutions and simplified administration of jointly delivered programmes (IES+Perto, 2016[51]).

Design quality assurance policies that support the effective use of digital technologies in teaching

Education systems need to develop a coherent quality assurance approach to digital education, as the use of digital technologies continues to expand in education systems. Incorporating a digital education dimension in quality assurance processes can support a more effective integration of digital technologies in teaching and learning.

School education systems rely on a range of quality assurance tools, including school self-evaluations, external evaluations, teachers and school leaders' appraisal, student standardised assessments and national qualifications/exams (European Commission, 2018[52]). Self-evaluation tools (e.g. the SELFIE tool developed by the European Commission) or a focus on digital technologies in external evaluation frameworks (European Commission/EACEA/Eurydice, 2019[18]) offer new avenues for monitoring and improving the use of digital technologies at the school level.

- With respect to the evaluation of education institutions themselves,
    - Already before the pandemic, in **Spain**, the Autonomous Community of Castilla y León included a comprehensive list of digital education-related indicators in its external school evaluation framework in order to evaluate the integration of digital technologies in teaching and learning activities (European Commission/EACEA/Eurydice, 2019[18]).
    - In **Ireland**, the implementation of the revised Digital Strategy for Schools to 2027 will include ongoing development of measurement and assessment mechanisms at the system level, combined with support for school self-evaluations and for teachers as part of their practices (Department of Education Ireland, 2022[53]). Prior to the revised Digital Strategy, some evaluation models in Ireland already enabled inspectors to assess schools' integration of digital technologies, for instance by examining whether schools relied on the Digital Learning Framework or had a Digital Learning Plan (European Commission/EACEA/Eurydice, 2019[18]).
- But quality assurance efforts also focus on the more granular level or actual digital education technologies. For instance in **Austria**, the 8-Point Plan for Digital Learning (launched in 2020 to support the goals of the pre-existing digital education strategy) includes a "Quality mark for learning apps" with the objective of encouraging an expansion in the availability of quality digital education resources and content (BMBWF, 2020[54]). Such apps will be subject to reviews and certification based on a range of criteria (education-related, ease of use, data privacy, etc.).

Given the diversification and multiplication of evaluation and assessment tools and methods, education systems need to ensure synergies among them to provide a coherent and consistent approach (OECD, 2013[55]). Building a coherent quality assurance approach for digital education therefore requires articulations between the different components of evaluation and assessment frameworks. In addition, capacity for quality assurance also needs to be built across education institutions, from teachers performing assessments of learning with digital technologies at the classroom level to school leaders or education administrators who rely on data to monitor, understand and assess the outcomes of education.

Quality assurance agencies should develop quality standards and guidance to inform higher education institutions to make innovative use of digital technologies, based on transnational guidance

In higher education systems, as mentioned previously, many institutions and governments base their quality assurance policies for digital education on guidance and standards produced by transnational organisations. The most recent ENQA Working Group "Considerations for the quality assurance of e-learning provision" (Huertas et al., 2018[22]) are not legally binding for quality assurance agencies and institutions operating in the EHEA, but propose a set of indicators that can be used to evaluate e-learning provision across each of the ten standards and guidelines of the ESG (Staring et al., 2022[56]). Quality assurance bodies and institutions may also draw on other international frameworks that provide indicators and methods for the quality assurance of digital higher education.

Following the guidance from transnational bodies, such as the common European approach to the quality assurance of digital higher education, national quality assurance bodies should seek to adopt quality standards and guidelines for digital higher education that can guide institutions to make innovative use of digital technologies. First, national quality assurance bodies should work with higher education stakeholders to develop a shared vocabulary for digital learning, informed by international frameworks, that builds common understanding and trust among higher education stakeholders and permits productive discussions about the scope for digital innovation in their higher education system.

- **Malta's** and **Romania**'s guidelines for digital higher education, for instance, both provide definitions for the wide variety of terms associated with digital learning (Malta Further and Higher Education Authority, 2021[57]; ARACIS, 2020[29]).
- In the **UK**, the Quality Assurance Agency for higher education has developed a *Taxonomy for Digital Learning* to "support providers to develop their ways of talking about digital methods of delivery, articulating what students can expect and therefore better assure themselves that quality and standards are being maintained" (QAA, 2020[58]).

Secondly, quality assurance agencies should collaborate with institutions to develop shared standards, indicators and methods for digital provision, covering all types of digitally enhanced education. Drawing upon leading international practice and national quality standards for digital higher education, potential indicators could be considered for the quality assurance of the following domains: institutional strategy for e-learning; digital education infrastructure, digital course design, delivery and assessment; staff professional development; student support and feedback; and monitoring and evaluation of outcomes.

- An example of a system that has developed national standards and guidelines in collaboration with the higher education sector is **Ireland**. In 2018 Quality and Qualifications Ireland (QQI) developed *Statutory Quality Assurance Guidelines for Providers of Blended Learning Programmes* (QQI, 2018[59]). In February 2022, QQI launched a call for tenders to revise the existing guidelines and expand their scope to fully online programmes.

Ongoing modernisation of quality assurance systems, across Europe in particular, can also support the development of new approaches for the quality assurance of digital education. Across Europe, many countries have been adapting their quality assurance systems in line with the European Commission's *Council Recommendation on building bridges for effective European higher education cooperation*, which states quality assurance systems should seek to "move further towards the use of institutional-based external quality assurance" and "allow for self-accreditation of programmes" (European Commission, 2022[60]).

- For example, **Hungary** is in the process of revising its programme accreditation procedures to make it easier for HEIs to launch new programmes, including in fully online and hybrid formats. Up to recently, Hungary's quality assurance system was characterised by heavy ex-ante programme accreditation procedures, based on a strict separation of programme types (full-time, part-time and distance learning) that have strict requirements on how these programmes are to be delivered by HEIs (Hungarian Ministry, 2011[61]). Ongoing reforms to the accreditation process are intended to support student choice and flexible learning, including the integration of digital study components such as asynchronous online learning into study programmes (OECD, 2023[62]).

Key messages

Digital education exposes learners to a variety of risks. Beyond the possible adverse effects of digital technologies on mental and physical well-being (e.g. extended screen time), these risks may also impact learners' human rights and children's' rights (e.g. inequitable access to education opportunities or data protection). Uses of advanced technologies such as AI in education contexts further amplify these concerns and call for regulatory efforts to protect learners in digital learning environments.

Currently, little specific regulation exists on the protection of learners in digital environments across OECD and EU countries. While broader regulatory frameworks – such as the GDPR – have implications for education institutions, more guidance and support are needed to empower education institutions to comply with these regulations. Specific regulations and guidance on the use of AI in education settings also remain largely absent from OECD and EU education systems.

The use of digital technologies also poses challenges on an institution level. For instance, the increasing use of digital learning tools makes education institutions more prone to cyber security threats. Some countries have promoted cyber security services specifically tailored to the needs of education institutions. Similarly, the broad variety of hardware and software used in education call for efforts to support interoperability of different tools to remove barriers to access to learning opportunities.

Beyond managing the challenges and risks associated with digital education, policy makers must assure the quality of digital infrastructure and pedagogies. Conventional quality assurance mechanisms – such as external evaluations or self-evaluation tools – must therefore be adapted to include aspects of digital education. Whilst the analysis in this chapter highlights that digital education is increasingly covered in quality assurance tools across OECD and EU countries, more attention needs to be paid to identify the relevant aspects of digital education which should be included in quality assurance frameworks.

References

1Edtech (n.d.), *Learning Tools Interoperability*, https://www.imsglobal.org/activity/learning-tools-interoperability. [46]

AARNet (n.d.), *Connectivity and collaboration services for K-12 schools*, https://www.aarnet.edu.au/k-12-schools (accessed on 12 April 2023). [39]

AARNet (n.d.), *Our Governance*, https://www.aarnet.edu.au/governance (accessed on 12 April 2023). [40]

ARACIS (2020), *Methodology and Guidelines on External Quality Evaluation in Higher Education in Romania. Part VI: Specific Standards and Guidelines on External Evaluation of the Quality of Distance Learning (DL) and Part-Time Learning (PTL) Degree Programmes*, ARACIS, Bucharest, https://www.aracis.ro/wp-content/uploads/2021/11/Result-1.-Part-VI-METHODOLOGY-DISTANCE-LEARNING-EN.pdf. [29]

Baker, R. and A. Hawn (2021), "Algorithmic Bias in Education", *Centre for Open Science*, https://doi.org/10.35542/OSF.IO/PBMVZ. [12]

BMBF (2021), *Erstes Pilotprojekt für Nationale Bildungsplattform startet - BMBF*, https://www.bmbf.de/bmbf/de/home/_documents/erstes-pilotprojekt-fuer-nationale-bildungsplattform-startet.html (accessed on 31 August 2022). [50]

BMBWF (2020), *Digitale Schule*, https://digitaleschule.gv.at/ (accessed on 5 December 2022). [54]

Bonefeld, M. and O. Dickhäuser (2018), "(Biased) Grading of Students' performance: Students' names, performance level, and implicit attitudes", *Frontiers in Psychology*, Vol. 9/MAY, p. 481, https://doi.org/10.3389/FPSYG.2018.00481/BIBTEX. [13]

Brown, M., N. Millichap and J. Dehoney (2015), "What's Next for the LMS?", *EDUCAUSE Review*, Vol. 50/4, https://er.educause.edu/articles/2015/6/whats-next-for-the-lms (accessed on 6 May 2022). [48]

Burns, T. and F. Gottschalk (eds.) (2019), *Educating 21st Century Children: Emotional Well-being in the Digital Age*, Educational Research and Innovation, OECD Publishing, Paris, https://doi.org/10.1787/b7f33425-en. [5]

Casovan, A. and V. Shankar (2022), *A framework to navigate the emerging regulatory landscape for AI - OECD.AI*, OECD. AI Policy Observatory, https://oecd.ai/en/wonk/emerging-regulatory-landscape-ai (accessed on 26 June 2022). [15]

CMS (n.d.), *GDPR Enforcement Tracker - list of GDPR fines*, https://www.enforcementtracker.com/ (accessed on 22 June 2022). [9]

Department for Education (2023), "Generative artificial intelligence in education", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1146540/Generative_artificial_intelligence_in_education_.pdf (accessed on 12 April 2023). [44]

Department for Education (2019), "Realising the potential of technology in education: A strategy for education providers and the technology industry". [33]

Department of Education Ireland (2022), *Digital Strategy for Schools to 2027*, https://www.gov.ie/en/publication/69fb88-digital-strategy-for-schools/#digital-strategy-for-schools-to-2027 (accessed on 26 August 2022). [53]

E4 Group (2015), *Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG)*, European Association for Quality Assurance in Higher Education; European Students' Union; European University Association; European Association of Institutions in Higher Education, http://www.enqa.eu/wp-content/uploads/2015/11/ESG_2015.pdf. [20]

Eduscol (2022), *Le référentiel CNIL de formation des élèves à la protection des données personnelles*, https://eduscol.education.fr/574/le-referentiel-cnil-de-formation-des-eleves-la-protection-des-donnees-personnelles (accessed on 27 June 2022). [30]

EUR-Lex (2016), *Document 32018R1725*, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552577087456&uri=CELEX:32018R1725 (accessed on March 2022). [6]

European Commission (2022), *Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators - Publications Office of the EU*, https://op.europa.eu/en/publication-detail/-/publication/d81a0d54-5348-11ed-92ed-01aa75ed71a1/language-en (accessed on 26 January 2023). [43]

European Commission (2022), *Proposal for a Council Recommendation on building bridges for effective European higher education cooperation*, European Commission, Brussels, https://education.ec.europa.eu/document/proposal-for-a-council-recommendation-on-building-bridges-for-effective-european-higher-education-cooperation (accessed on 24 June 2022). [60]

European Commission (2022), *The European Interoperability Framework in detail*, https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail (accessed on March 2022). [16]

European Commission (2018), *etter learning for Europe's young people : developing coherent quality assurance strategies for school education : report from an expert assignment*, https://data.europa.eu/doi/10.2766/86303 (accessed on 23 February 2023). [52]

European Commission/EACEA/Eurydice (2019), *Digital Education at School in Europe*, Eurydice Report. Luxembourg: Publications Office of the European Union, https://eacea.ec.europa.eu/national-policies/eurydice/content/digital-education-school-europe_en (accessed on 4 August 2020). [18]

European Union (n.d.), *Europass digital credentials*, https://europa.eu/europass/digital-credentials/issuer/#/home. [47]

FELVI (2021), *Statistics from the past years of applications and acceptence (2001-2021*, https://www.felvi.hu/felveteli/ponthatarok_statisztikak/elmult_evek/!ElmultEvek/index.php/elmult_evek_statisztikai/munkarendenkent (accessed on March 2022). [26]

Gaebel, M. et al. (2021), "DIGITALLY ENHANCED LEARNING AND TEACHING IN EUROPEAN HIGHER EDUCATION INSTITUTIONS", http://www.eua.eu (accessed on 7 December 2021). [25]

Géant (2020), *Compendium of National Research and Education Networks in Europe - 2020*, https://about.geant.org/wp-content/uploads/2021/12/Compendium_FINAL2.pdf. [8]

GOV.UK (2021), *Quality assuring providers of full-time online education*, https://educationinspection.blog.gov.uk/2021/11/24/quality-assuring-providers-of-full-time-online-education/ (accessed on 1 September 2022). [19]

Grand View Research (2021), *AI In Education Market Size & Share Report, 2022-2030*, https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-education-market-report/methodology (accessed on 26 January 2023). [41]

Holmes, W. et al. (2022), "Artificial Intelligence and Education: A critical view through the lens of human rights, democracy and the rule of law", http://book.coe.int (accessed on 7 April 2023). [10]

Huertas, E. et al. (2018), *Considerations for quality assurance of e-learning provision*, European Association for Quality Assurance in Higher Education, Brussels, https://www.aqu.cat/elButlleti/butlleti91/articles2_en.html#.YGY_R5NKhTZ (accessed on 22 December 2021). [22]

Hungarian Ministry (2011), *Act CCIV of 2011 on National Higher Education*. [61]

IES+Perto (2016), *IES+Perto project results*, https://iesmaisperto.up.pt/?page_id=147. [51]

INQAAHE (2022), "International Standards and Guidelines for Quality Assurance in Tertiary Education 2022 Edition © International Network for Quality Assurance Agencies in Higher Education", https://www.inqaahe.org/sites/default/files/INQAAHE-International-Standards-and-Guidelines-ISG.pdf (accessed on 19 February 2023). [23]

INQAAHE (2018), *Guidelines of Good Practice*, International Network for Quality Assurance Agencies in Higher Education (INQAAHE), Barcelona, https://www.inqaahe.org/guidelines-good-practice (accessed on 10 January 2022). [21]

International Working Group on Digital Education (2016), "Référentiel de Formation des élèves à la protection des données personnelles". [31]

Malta Further and Higher Education Authority (2021), *Guidelines for Quality Assurance - For Online Learning Providers in Malta*, Malta Further and Higher Education Authority, Valletta, https://mfhea.mt/wp-content/uploads/2021/10/Guidelines-for-FHEI-V1.pdf (accessed on 2 August 2022). [57]

Ministère de l'éducation nationale (n.d.), *Le Gestionnaire d'Accès aux Ressources (GAR)*, https://eduscol.education.fr/213/gestionnaire-d-acces-aux-ressources (accessed on 3 April 2023). [32]

NCSC (2021), *Cyber Security for Schools*, https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools (accessed on 27 June 2022). [34]

Netjogtar (2022), *Updated Government Decrees*, https://net.jogtar.hu/. [27]

NSIP (n.d.), *The National Schools Interoperability Framework*, https://www.nsip.edu.au/about-nsip. [49]

OECD (2023), *Advancing Digital Maturity in Croatia's Higher Education System*, OECD Publishing, Paris, https://doi.org/10.1787/26169177. [28]

OECD (2023), *Ensuring Quality Digital Higher Education in Hungary*, Higher Education, OECD Publishing, Paris, https://doi.org/10.1787/5f44fd6f-en. [62]

OECD (2022), *Companion Document to the OECD Recommendation on Children in the Digital Environment*, OECD Publishing, Paris, https://doi.org/10.1787/a2ebec7c-en (accessed on 1 September 2022). [4]

OECD (2021), "Children in the digital environment: Revised typology of risks", *OECD Digital Economy Papers,*, No. 302, OECD Publishing, Paris, https://doi.org/10.1787/9b8f222e-en (accessed on 1 September 2022). [2]

OECD (2021), *OECD Digital Education Outlook 2021: Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots*, OECD Publishing, Paris, https://doi.org/10.1787/589b283f-en. [11]

OECD (2021), *Recommendation of the Council on Children in the Digital Environment*, OECD Legal Instruments, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389%20 (accessed on 28 June 2022). [36]

OECD (2021), *Supporting the Digital Transformation of Higher Education in Hungary*, Higher Education, OECD Publishing, Paris, https://doi.org/10.1787/d30ab43f-en. [37]

OECD (2020), "Protecting children online : An overview of recent developments in legal frameworks and policies"*, OECD Digital Economy Papers*, No. 295, OECD Publishing, Paris, https://doi.org/10.1787/9e0e49a9-en (accessed on 27 June 2022). [1]

OECD (2019), *The OECD Artificial Intelligence (AI) Principles - OECD.AI*, https://oecd.ai/en/ai-principles (accessed on 31 May 2023). [45]

OECD (2013), *Synergies for Better Learning: An International Perspective on Evaluation and Assessment*, OECD Reviews of Evaluation and Assessment in Education, OECD Publishing, Paris, https://doi.org/10.1787/9789264190658-en. [55]

Perry, A. and N. Turner-Lee (2019), *AI can disrupt racial inequity in schools, or make it much worse*, https://hechingerreport.org/ai-can-disrupt-racial-inequity-in-schools-or-make-it-much-worse/ (accessed on 31 May 2023). [14]

QAA (2020), *Guidance Building a Taxonomy for Digital Learning*, Quality Assurance Agency for Higher Education (QAA), London, https://www.qaa.ac.uk/docs/qaa/guidance/building-a-taxonomy-for-digital-learning.pdf (accessed on 31 July 2020). [58]

QQI (2018), *Statutory Quality Assurance Guidelines for Providers of Blended Learning Programmes*, Quality and Qualifications Ireland (QQI), Dublin, https://www.qqi.ie/sites/default/files/media/file-uploads/Statutory%20QA%20Guidelines%20for%20Blended%20Learning%20Programmes.pdf (accessed on 8 December 2021). [59]

République Française (2020), *Référentiel général d'interopérabilité (RGI)*, https://www.numerique.gouv.fr/publications/interoperabilite/ (accessed on 2022). [17]

Ruohonen, J. and K. Hjerppe (2022), "The GDPR enforcement fines at glance", *Information Systems*, Vol. 106, p. 101876, https://doi.org/10.1016/J.IS.2021.101876. [7]

SIVON (2022), *SIVON behartigt belangen schoolbesturen*, https://www.sivon.nl/sivon-behartigt-belangen-schoolbesturen/ (accessed on March 2022). [38]

Staring, F. et al. (2022), *Digital higher education: Emerging quality standards, practices and supports*, https://www.oecd.org/education/digital-higher-education-f622f257-en.htm. [56]

Tait, A. (2022), *ICDE Quality Network report 2021: Global Quality Perspectives on Open, Flexible and Distance Learning 2021 — ICDE*, ICDE, Oslo, https://www.icde.org/knowledge-hub/icde-quality-network-report-2021 (accessed on 24 June 2022). [24]

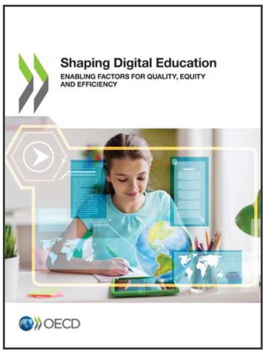
Turner Lee, N., P. Resnick and G. Barton (2019), *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/#footref-38 (accessed on 26 January 2023). [42]

UNICEF (2022), *Child Online Protection in and through Digital Learning*, UNICEF Regional Office for Europe and Central Asia (ECARO). [3]

US Department of Education (n.d.), *Protecting Student Privacy*, https://studentprivacy.ed.gov/ (accessed on 12 April 2023). [35]

Notes

[1] The *standards* are defined as “agreed and accepted practice for quality assurance in higher education in the EHEA”; the *guidelines* explain “why the standard is important and describe how standards might be implemented”, setting out examples of good practice (E4 Group, 2015, p. 9[20]).


Shaping Digital Education
ENABLING FACTORS FOR QUALITY, EQUITY AND EFFICIENCY
OECD

From:

Shaping Digital Education

Enabling Factors for Quality, Equity and Efficiency

Access the complete publication at:
https://doi.org/10.1787/bac4dc9f-en

Please cite this chapter as:

OECD (2023), “Guidance and regulatory frameworks for digital education”, in *Shaping Digital Education: Enabling Factors for Quality, Equity and Efficiency*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/a0a23dc6-en

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.