

Education Sector Aide-Mémoire[#]

Global Digital Collaboration Conference 2026

1-3 September 2026 | Geneva, Switzerland

1. The Global Digital Collaboration ([GDC](#)) on credentials and wallets advances dialogue to support trusted and interoperable digital public infrastructure worldwide. Together with the World Bank, Linux Foundation and other cross-sector partners, UNESCO's Education Sector is one of 40 council members and co-organizers of the GDC2026 conference, hosted by the Swiss Confederation.
2. GDC2026 focused on the *infrastructure of digital trust*, including: digital identity and digital wallets; verifiable credentials; interoperability and standards; trust, governance and regulation; and moving from standards to real-world use cases.
3. Education sector contributions at GDC2026 included a keynote address on recognizing and sharing learning achievements, as well as various panels focusing on: verifiable credentials and academic recognition: building global trust for lifelong learning; scaling trust: sovereign digital public infrastructure for research, education and innovation in Africa; cross-border data sharing for learner mobility and credential recognition; building digital public infrastructure for education systems with verifiable credentials; and the role of research and technology organisations.
4. Observations relevant for the education sector from the GDC2026:
 - a. *Overarching*
 - i. Global digital credentialing ecosystems are developing at an extraordinary pace driven by AI and commercial interest. There is a risk that education as a human right and public good will be negatively impacted, increasing the digital divide, if the sector is too slow in responding to these new developments. There is a need to ensure inclusiveness including ensuring the global South in general and Africa specifically is involved in these developments.
 - ii. Digital identity and other credentials contained in digital wallets contain a range of credentials including learning credentials and used for travel, banking, study, employment, accessing social and health services etc. Learning credentials, by-and-large, require similar standards, protocols, APIs, wallets and other open source technological tools. This provides an opportunity for the education sector to utilise existing tools without the need to develop them from scratch.
 - iii. At this point few education systems, more so public education systems, are playing an active role in the development and deployment of the new credentialing infrastructure that has become mainstream in many other sectors. Examples include health, driving licenses and passports.
 - iv. Governance is the constraint on scale across sectors, not technology. This point was made by participants from aviation and trade. It is imperative that governance is settled before technology determines the ecosystem. The risk for education is that a governance system that comprehensively addresses digital credentials arrives after the technology ecosystem has already determined the rules. There is opportunity to build the technical understanding and capacity of legacy educational institutions that already play a critical role in governing traditional skills qualifications.
 - v. There is also an urgent need for civil society, academia, and experts from the education ecosystem to air their concerns so such credentialing systems are not driven purely by the interests of technology service providers and private actors and are instead developed in public interest.
 - vi. Credentialing systems must not only be digital by design but also human-centric. Human centred approaches must be manifested in both technical frameworks and governance

systems, and must be developed in consultation with the range of user groups within the education ecosystem, such as learners, administrative officials, verifying entities, and accrediting institutions co-creation sessions through the various stages of design and development, and the implementation of robust grievance redressal mechanisms are critical in ensuring that multi-stakeholder feedback is regularly and meaningfully addressed. As an example, learners who receive a European Digital Credential (EDC) have full control over their personal information. EDCs are issued to learners via email or by direct deposit into their wallet. From there, learners can choose how and when to share their credentials with third parties via share-links or PDF export and for how long.

- vii. Credentialling frameworks that are only built on formal economy assumptions exclude vast populations whose work and learning reside in informal/non-formal areas and therefore fall outside formal recognition structures. Recognition of prior learning is the instrument that allows entry of informally acquired competence to enter a verifiable credentialling system. While such recognition is a separate matter to the development of digital credentialing infrastructure, it is nevertheless important and appropriate systems should ideally be also developed.
- viii. Credential frameworks would also benefit from expanding beyond the formal higher education system, to include co-curricular qualifications and skills acquired in the workplace, among others.

b. *Digital identity and digital wallets*

- i. The fragmentation of digital identity systems poses a risk to systems and countries, creating additional vulnerabilities for children and disadvantaged communities.
- ii. There are a number of commercial providers developing digital wallets. Countries need to consider whether more standardised wallets should be developed through a national system, or even through regional and continental systems. As an example, the EU Digital Identity (eID) Wallet will enable users to access online and offline public and private services, store and share digital documents, and create binding signatures. Europass, on the other hand, already readily offers a free wallet service that is able to receive and store learning credentials, including EDCs.

c. *Verifiable credentials (VCs)*

- i. Prominent standards and specifications for VCs include W3C VC (domain neutral data model), ISO mdoc (used mainly for mobile driving licences and identity credentials) and SD-JWT VC (allowing for selective disclosure), and the European Learning Model (ELM).
- ii. The landscape of badges, skills passports, Digital diplomas, transcripts, learning and employment records, micro-credentials and qualifications have not yet developed into an ecosystem. Significant gaps with regard to interoperability, transferability and therefore value and trust remain, although mapping activities are undertaken by representatives of W3C VC, Open Badge, Credential Transparency Description Language (CTDL) and ELM standards.
- iii. While verifiable credentials promise frictionless learning and workforce mobility, bridging fragmented regional and national standards, data privacy laws, and trust frameworks remains a complex challenge. Since the technical architecture of verifiable credentials will spawn parallel ecosystems of issuers, verifiers, wallets and trust registries, considerations will need to be made around agencies that will coordinate these data-sharing functions, business models for adoption and sustainability and long-term investments that are required to transition from legacy systems to verifiable digital ecosystems.
- iv. There is also a need to think about barriers to effective VC use among relevant actors and how we might bridge these gaps. For instance, adopting a VC credential architecture will require increased technical capacity at and some financial investment from educational institutions. Adoption also presumes sufficient data literacy and access to the internet, ideally by smartphone but otherwise by a desktop device, and may deepen the digital divide for marginalised groups.

d. *Interoperability and standards*

- i. Rich metadata should be a strategic focus for inclusion in credential descriptions in order to support interoperability and the emerging digital infrastructures. Sample European Digital Credentials (e.g. micro-credential) that demonstrate such data richness, are published in the [ELM Support GitLab](#).
- ii. Credential interoperability can also be supported by making the credential metadata multilingual, and by utilising multilingual controlled vocabularies and linked open data, that allows mapping skills taxonomies and competence frameworks to each other. As an example, the European Learning Model uses a wide range of standard vocabularies, including a collection of controlled lists of simplified, re-usable and extensible collections of multilingual labels.
- iii. The UNESCO-UNICEF-ITU [Charter for Public Digital Learning Platforms](#) clarifies purposes for digital learning platforms and recommends seven principles to guide their development and governance. Digital credentials, and wallets, are not the same as, but are adjacent to, such platforms. Accordingly, the principles may need extension or adaptation.

e. *Trust, governance and regulation*

- i. A learner-centred approach supported by shared standards is needed to build trust and ensure recognition of digital and verifiable credentials worldwide. It is important to distinguish between the various trust flows at play within this ecosystem and which should take priority. To offer an example, there is the trust learners may or may not hold towards educational institutions and trust in the digital wallets that enable data exchange which has significant bearing on rates of adoption. Separately, there is also the trust verifying entities may or may not place in the credentials being shared with them which influences their buy-in.
- ii. An open infrastructure for education and workplace digital credentials will contribute to a trust framework that provides the foundation for a wide variety of applications to be developed in a marketplace.
- iii. If the UNESCO [Global Convention](#) is to support lifelong and life-wide learning in the age of global digital collaboration, it will need to strengthen its connectivity with employment supported by work on competency frameworks, and on more seamless connections between education and employment. ESCO is an exemplary extensive European taxonomy, where multilingual occupation concepts (e.g. "nurse responsible for general care") are linked to multilingual essential and optional skill and competence concepts (e.g. "apply person-centred care").
- iv. National and regional qualifications frameworks, and their mapping on linked open data level, can provide an important reference point for digital trust registries that are able to interface with industry/employer facing systems, and also the wide variety of other non-education credentialing systems. The Irish NQF is an example where NQF levels have been mapped to EQF levels, and vice versa, on RDF data level.
- v. Emerging work on delegated AI authority (AI agents acting on behalf of human beings) is being spearheaded and standardised by groups such as EMVCo, FIDO Alliance and the Linux Foundation. These decisions have implications for how learner-held credentials are shared and used. The education sector must establish a position on consent and learner ownership before the standards are established.

f. *Moving from standards to real-world use cases*

- i. There are opportunities to learn from the capacity building challenges and need for sustainability of a suitably skilled workforce through examples such as [DIGITAfrica](#). DIGITAfrica has established the technical layer for open architecture, sovereign DPI through cooperation across 5 African universities, while establishing mutual recognition of a digital credential for participating researchers and students within the project framework.

- ii. The Groningen Declaration Network ([GDN](#)) provides an important interdisciplinary network of networks that supports the specific cross sectional work between education and digital infrastructure developments.
- iii. Velocity Network Foundation ([VNE](#)) is a global non-profit membership organization, of technology vendors and solution providers, which has established and democratically governs a trust framework for the digitization, issue and exchange of credentials originally issued on paper, and their subsequent digital verification by relying parties, such as employers. Velocity's current emphasis is on credentials required for work, rather than on the issue of qualifications as verifiable digital credentials directly by learning providers.
- iv. National Qualifications Registries are existing authoritative sources of trust and may be a starting point in some countries, but would require wallets to contain proof of ID before use in education. If this route is chosen, the task will be to ensure existing registers become digitally verifiable instead of building new platforms.
- v. Human Rights for Digital Identity Coalition ([HR4ID](#)) provides a common position on the potential harms posed by different types of digital ID systems and mandatory requirements, highlight the positive and negative obligations of public and private institutions, and make recommendations for designing systems that will help to ensure human rights.
- vi. The [California Career Passport Program](#) is a state-level initiative intended to give individuals a secure digital record of education, skills, credentials and experience that they can share with employers.
- vii. Indonesia has developed a national infrastructure for qualification verification through its [PDDikti](#) national higher-education database connected to the PISN (National Diploma and Professional Certificate Numbering) system, through which diploma and professional-certificate numbers can be checked against national higher-education records.

As the education sector participants in GDC2026* we call on the education sector actors to take a more proactive role in building a global infrastructure for digital trust that is based on the principles of: upholding and fulfilling the human right to education; governed as digital public goods; and strengthened inclusion, equity, safety, and quality across education systems as outlined in the UNESCO Charter for Public Digital Learning Platforms.

Education sector actors nationally and globally should not be passive participants in this massive global shift. We need to be active contributors that are able to engage technically on an equal footing, while providing guardrails for the global infrastructure for digital trust.

3 September 2026

#Disclaimer: This aide memoire has been drafted collectively by the education sector participants that attended GDC2026. The views expressed are of the individuals and do not necessarily represent any specific organisational views.

*Education sector invitees and participants: Antara Madavane; Armando Manzueta; Cheikh Bamba Gueye; Chiara Finocchietti; Damien Saucez; Etan Bernstein; Fortunate Benda; Ildiko Mazar; Iwan Fathony; James Keevy; Joanne Duklas; John Harrison; Jorge R Tort; Joyce Mwangama; Luca Lantero; Madhuchandra R; Makhapa Makhafola; Ndahiro Moses; Norda Seymour-Hall; Paulina Pannen; Phumudzo Silimela; Raffaele Bruno; Rahayu Riyanti; Rachel Scherer; Rohan Pai; Rupert Ward; Serge Ddida; Sharon Leu; Susanna Karakhanyan; Vitalis Ozianyi; Weaam Zaghloul; Whitfield Green; and Winnie Karanu.