

ENC ANALYSIS

ENC
ENCouncil.org
European Neighbourhood Council

A Digital Duty of Care: Protecting the Data of Afghan Girls in Online Education

NOVEMBER 2026

Authors
Nematullah Akbari
Dr. Rashid Gabdulhakov

Table of Contents

About the Authors
Summary
Executive Summary
Key Recommendations
Problem Analysis
Evidence and Threat Model
Relevance to EU Policy
Policy Options
Recommended Course of Action
Implementation Timeline
Conclusion
References

About the authors



Nematullah Akbari is currently an MA student in Politics and Security (Central Asia) at the OSCE Academy in Bishkek, Kyrgyzstan. He is writing his MA thesis on the political functions of the Taliban's gendered system of governance, which he dedicates to the Afghan women and girls resisting Taliban rule. His research interests include the politics of Afghanistan and Central Asia, the New Great Game amid evolving geopolitics, and gendered political systems in the 21st century. Through his work, he aims to highlight the dedication and resilience of those who advocate for equity, justice, and accountable political systems, particularly in developing countries.



Dr. Rashid Gabdulhakov is an Assistant Professor at the Research Centre for Media and Journalism Studies at the University of Groningen, the Netherlands, and a member of the ENC Academic Council. His current research focuses on the role of social media in informing and disinforming online communities of Central Asians in Russia and Russophone communities in Europe, with a broader commitment to highlighting people, places, and cases that remain underrepresented in scholarly debates.

Executive Summary

Online education has become one of the few remaining ways for Afghan girls and women to continue learning since the Taliban barred them from secondary schools and universities. Since 2021, dozens of Afghan-led, diaspora-led, and international initiatives have helped move the learning process online, with the use of phones, laptops, and messaging apps. This progress carries a hidden cost: every enrolment, message, and login leads to a digital trace that puts those already vulnerable into greater danger of state retaliation.

Online education is not genuinely safe when participation creates identifiable digital traces that may expose learners, teachers, and their families. The EU Delegation to Afghanistan should therefore treat data protection as part of its responsibility to ensure that the education programmes it funds do not expose participants to avoidable harm. This is a policy and funding-based duty of care, rather than a claim that EU data-protection law automatically applies to every Afghan provider. The GDPR applies only where the territorial conditions in Article 3 are met, while the Digital Services Act (DSA) applies to intermediary services offered to recipients located in the EU; EU funding alone does not bring an Afghan-only education provider within either instrument's scope. The practical case for EU action is more direct: the Delegation can set proportionate safeguards in its own grant agreements, drawing on EU data-protection principles and relevant international child-protection standards.

The European Union has maintained an operational presence in Kabul since shortly after the Taliban's return to power in August 2021, led by a Chargée d'Affaires rather than an accredited ambassador, under a policy of "operational engagement" set out in the Council Conclusions of September 2021 and March 2023 (EEAS, 2026). Without recognising or legitimising the Taliban-run de facto authorities, the Delegation manages EU support for healthcare, education, and humanitarian aid, channelled exclusively through UN agencies, international NGOs, the Red Cross/Red Crescent, and the World Bank Group under a "by women, for women" principle, with no funds passing through Taliban structures (EEAS, 2026). Five years on, the EU describes itself as one of the few remaining Western diplomatic presences in the country — a position that gives the Delegation both the

funding relationships and the standing to embed data-protection conditions into the programmes it funds.

Most providers currently operate without mandatory data-protection standards, dedicated funding for secure systems, or accountability from the commercial platforms they depend on. This assessment rests on two observations. First, independent analysis has found that the major platforms these providers depend on, including Meta and Google, have not built privacy-by-default protections tailored to the Afghan context; even a March 2026 Meta Oversight Board recommendation was limited to excluding high-risk regions from a single feature rather than establishing a binding data-protection standard (Bouachrine, 2026). Second, a review of publicly available material for this brief did not locate a published data-protection policy for any of the Afghan-led or diaspora-led providers mapped in this brief — which is precisely why Recommendation 2 calls on the Delegation to commission a systematic review to confirm this directly with providers. This brief recommends that the Delegation treat data protection as a core condition of the education and humanitarian funding it manages — not an optional add-on — and pair that standard with practical, funded support so that small and under-resourced providers can meet it.

Key Recommendations

The EU Delegation to Afghanistan should:

Within three months, add minimum data-protection and digital-safeguarding requirements to every new or renewed grant managed by the EU Delegation that supports online education for Afghan girls and women.

Within three months, commission a rapid review of data-handling practices among online education providers it funds or may fund. The review should examine systems and procedures—not collect or centralise the identities of individual learners or teachers.

Within nine months, establish, with interested Member State missions present in the region, a pooled technical-assistance facility so smaller providers can meet the new standards rather than being excluded by them.

Ongoing: Raise data-minimization and account-security features for high-risk Afghan users through the Delegation's channel to EEAS Headquarters for engagement with Meta/WhatsApp and other relevant platforms.

Within 24 months, provide funding for low-bandwidth and offline-capable learning tools and support providers in moving, where feasible, away from real-name registration. These measures should help providers meet the standards above, not replace them.

Problem Analysis

Afghanistan is the only country in the world where girls are formally barred from secondary and higher education. Since the Taliban returned to power in August 2021, an estimated 2.2 million adolescent girls have been denied access to secondary school (UNESCO/UNICEF, 2026). This number is escalating every year as those graduating six grades will automatically be barred from further education. Since the access to secondary and higher education for girls has been prohibited. through official decree denounced by the Taliban de-facto authorities, online education leaves blind spot in the plight of women's access to education.

“The internet was the only thing we had left,” said one Afghan woman attending online classes, describing what it meant to lose access even to that (Feminist Majority Foundation, 2025).

Against this backdrop, online education has become one of the few remaining ways for Afghan girls and women to continue learning. Eagle Online Academy, a Virginia-based nonprofit founded in 2019 by Mozhgan Wafiq Alokozai and sustained mainly through individual donations and fundraising events rather than government or institutional grants, reports having graduated more than 2,000 women and girls since 2020 (Eagle Online Academy, 2026). SOLAx, a WhatsApp-based academy launched by the School of Leadership, Afghanistan, in 2024, has enrolled more than 29,000 students (8am Media, 2026). Anar Academy allows students to enrol under pseudonyms to help protect their identities. These initiatives represent significant achievements under extraordinary constraints. Other civil-society organisations have also adapted their work to provide online learning, often using widely available tools such as Google Meet, Zoom, and WhatsApp. However, the security and data-handling practices of these programmes vary, and publicly available information remains limited.

Yet a critical blind spot remains largely unaddressed: when a girl enrolls in an online course, she leaves behind a trace — her name, her location, contact details, attendance record — collected by providers as a routine administrative act, in most cases without a clear data-protection policy, encryption standard, or breach-response plan. Online education is not genuinely safe if participation itself creates a record that could later expose the learner, her teachers, or her family. This is the core problem the Delegation is positioned to help address, and the reason a digital duty of care should sit alongside access to education in its funding decisions.

On this specific point, no publicly documented case yet ties a breach of an online course's enrolment database to a specific instance of retaliation. Related evidence is, however, documented at the level of individual devices: Taliban authorities have used prohibited material found on phones searched at checkpoints as grounds for detention (Human Rights Watch, 2026), and Afghanistan's new Criminal Procedure Code, in force since January 2026, empowers male relatives and community members to report women and girls for offences that include "secretly accessing education online," extending the risk of exposure into the household (Bouachrine, 2026). These findings support treating exposure through digital traces as a credible risk consistent with this brief's threat model, even though a case specifically involving a breached learner database has not yet been documented.

Evidence and Threat Model

The online-education ecosystem

Providers reaching Afghan girls range from small Afghan-led initiatives to diaspora-founded nonprofits and, indirectly, large commercial platforms:

- Diaspora-led and Afghan-led nonprofits, such as Eagle Online Academy, SOLA/SOLAx, Anar Academy, Begum Academy, and Banoo Online School, deliver curricula by website, app, or messaging platform, often free of charge.
- Delivery frequently depends on commercial, general-purpose platforms — most notably WhatsApp — that were not designed for a population under active surveillance risk and are not subject to any Afghanistan-specific safeguarding agreement.
- Scale varies widely, from a few hundred to tens of thousands of learners per provider (for example, SOLAx reports more than 29,000 enrolments since 2024).

EU support identified for Afghan education in the sources reviewed for this brief includes a €140 million basic-needs and livelihoods package announced in September 2023, a €25 million contribution to UNICEF for primary-school education, and a €6 million grant to Save the Children announced in September 2025. The €25 million UNICEF education project is described as a two-year project; the public announcement for the €140 million package does not specify one implementation period for the entire package, and the cited €6 million announcement does not state a project duration. These are

dated funding announcements, not evidence of one continuing allocation. The public sources reviewed did not identify comparable EU funding specifically earmarked for the data protection or digital safety of online education providers. This apparent gap, rather than an absence of need, is the policy issue addressed here.

What is documented

Several facts relevant to this brief are well documented and should anchor the analysis:

- The Taliban's morality police and intelligence services have raided homes used for underground, in-person girls' schooling and detained teachers, including in a wave of raids reported in late 2025 (EUAA, 2025; Human Rights Watch, 2025; KabulNow, 2026).
- In September 2025, the Taliban imposed a nationwide shutdown of fibre-optic and mobile internet services across all 34 provinces, later partially reversed — demonstrating both the capability and the willingness to control digital access at scale (Human Rights Watch, 2025).
- Several individuals involved in providing online education content have been detained for the nature of their material (KabulNow, 2026).

Public reporting reviewed for this brief did not identify a documented case in which the Taliban breached the specific enrollment database of an online learning platform. That absence of evidence is not evidence of safety: it may reflect limited independent investigation of a closed environment as much as an absence of risk. Given the demonstrated willingness to target underground and in-person education and to restrict digital infrastructure, the responsible planning assumption is a credible risk rather than either a confirmed practice or a purely hypothetical one:

Insecure learner records could enable the identification, intimidation, detention, or coercion of students, teachers, and their families.

This brief distinguishes between documented incidents, credible risks supported by demonstrated capability and intent, and possible but currently unsubstantiated scenarios, and recommends that any future revision update this assessment as new evidence emerges.

How learners could be exposed: a threat model

The risks facing online learners are not limited to sophisticated state hacking. Most stem from ordinary operational gaps operating in a hostile environment:

- Collection of more personal data than a course requires
- Real-name registration instead of pseudonyms or ID codes
- Shared or confiscated household devices
- Weak or reused passwords and phishing
- Visible notifications, contact lists, or group chats on a shared device
- Learner records kept in poorly secured spreadsheets or cloud folders
- Insider access by staff or volunteers without vetting or access controls
- Long retention of records after a course ends
- Data collection by third-party platforms (e.g. messaging apps) outside the provider's control
- Internet shutdowns and telecommunications monitoring at the network level

A layered response has to address this full range of vectors, not just the most technically dramatic ones.

The limits of technical fixes

Signal, encryption, and VPNs can reduce specific risks, but none of them constitutes a complete solution, and the Delegation should not present them as such when funding technical assistance:

- A secure messaging app does not protect a device that is confiscated or inspected while unlocked.
- VPN use may itself be restricted or draw attention in some contexts.
- Metadata (who messaged whom, when, how often) can reveal patterns even when message content is encrypted.
- Backups, notifications, and saved contact lists can expose users even when the core app is secure.
- Internet shutdowns can make any digital tool unusable regardless of how well it is secured.

Recommendations in this brief therefore call for a layered, context-specific approach based on risk assessment, rather than prescribing a single application as a fix for every provider.

Relevance to EU Policy

The EU Delegation to Afghanistan is well placed to act on this issue for several concrete reasons:

• Funding relationships: the EU has a substantial record of supporting Afghan basic needs and education. Examples include the €140 million package announced in September 2023, education support through UNICEF, and a €6 million grant to Save the Children announced in September 2025. These figures refer to specific funding announcements made in different years. The UNICEF education project is described as lasting two years, while the cited €140 million package announcement does not give a single implementation period for the whole package and the €6 million announcement does not state a duration. They should not be read as one ongoing fund or as proof that the Delegation currently controls every related grant. The relevant point is that the EU has established funding relationships through which future agreements can include proportionate safeguards.

• Policy mandate: EU external action places gender equality and women's and girls' rights among its stated priorities, giving the Delegation a clear policy basis for treating digital safety as integral to — not separate from — the right to education.

• Access to data-protection expertise: the Delegation can draw on EU data-protection principles, the GDPR, and international child-online-protection guidance when designing proportionate safeguards. This does not mean that the GDPR automatically applies to every Afghan provider: Article 3 sets territorial conditions, including processing in the context of an EU establishment or certain processing involving people in the EU. Similarly, the DSA applies to intermediary services offered to recipients located in the EU, not simply because an activity is supported by EU funds. These instruments can inform the standards used in funding agreements without overstating their direct legal reach in Afghanistan.

- Grant conditionality: agreements negotiated or overseen by the Delegation can require minimum safeguards as a condition of support, a lever not readily available to most other actors on the ground.

- Convening role: the Delegation already coordinates with other donor missions present in the region on Afghanistan policy, and can use that role to align data-protection expectations across donors and refer platform-level concerns to EEAS Headquarters.

Taken together, these factors give the Delegation a credible basis for action, but they do not establish a blanket legal duty under EU data-protection law to regulate every Afghan online education provider. The stronger and more practical argument is that the EU already chooses which programmes it funds, has committed to protecting women's and girls' access to assistance, and can make reasonable safeguards a condition of its own grants. Where EU-supported education creates foreseeable data risks, a proportionate digital duty of care follows from responsible programme design and the principle of avoiding harm. It should be implemented with Afghan educators and providers, and paired with technical support so that safeguards improve protection rather than exclude smaller initiatives.

Policy Options

The following three options address the data-protection gap at different levels of urgency and scope. They are complementary rather than mutually exclusive, and this brief recommends the Delegation pursue them together rather than choosing a single track.

Option A: Mandatory Minimum Data-Protection Standards

The Delegation would require, in grant agreements it negotiates or oversees, minimum safeguards for any online education initiative it funds: pseudonymous or ID-code registration, no unnecessary collection of location data, encryption of records, data minimization, and deletion of learner records on a defined schedule. This would draw on UNICEF's Policy on Personal Data Protection and the UNICEF/ITU Guidelines for Industry on Child Online Protection, and on relevant Commission-level guidance.

Strength**:** addresses the root governance gap directly and is enforceable through funding agreements the Delegation already manages.

Limitation: providers entirely outside the Delegation's funding relationships may not comply without added incentives or technical support.

Option B: Targeted Technical and Financial Assistance

The Delegation would fund smaller providers in adopting safer, low-bandwidth, and offline-capable systems, and in migrating away from real-name registration, building on models already piloted by providers such as Anar Academy.

Strength: provides concrete, near-term protection to girls learning now, and makes compliance with Option A achievable for under-resourced providers.

Limitation: internet shutdowns can disable even well-secured infrastructure, and technical tools alone cannot fix weak data governance.

Option C: Platform Accountability Engagement

The Delegation would refer the issue to EEAS Headquarters to convene major platforms reaching Afghan learners — including Meta (WhatsApp), Khan Academy, Coursera, and FutureLearn — alongside other donor governments and civil society, to secure voluntary, publicly stated commitments on data handling for users in high-risk contexts.

Strength: creates durable change across the full ecosystem, including large commercial platforms outside the Delegation's direct funding relationships.

Limitation: complex and slow, and outside the Delegation's direct authority; a medium-to-long-term measure that cannot substitute for the more immediate steps in Options A and B.

Recommended approach: use Option A as the backbone — mandatory standards attached to Delegation-managed funding — paired with Option B so that smaller providers can realistically comply, and initiate Option C as a parallel, medium-term track led jointly with EEAS Headquarters.

Recommended Course of Action

1. Set minimum data-protection standards

Within three months, the Delegation should introduce minimum data-protection and digital-safeguarding conditions into all new and renewed grants it manages that support online education for Afghan girls and women. Compliance should be assessed at grant renewal through a lightweight self-certification plus spot-check model, not a full audit, so as not to exclude small providers.

2. Commission a system-level review

Within three months, the Delegation should commission a rapid review of data-handling practices across the online education providers it funds or is likely to fund — covering what data is collected, where it is stored, who can access it, retention periods, and breach-response readiness. The review should map providers' systems and procedures only, and must not collect or centralize the identities of individual learners or teachers.

3. Build a shared technical-assistance facility

Within six to nine months, the Delegation should work with interested EU Member State missions present in the region to co-finance a shared technical-assistance facility, administered by UNICEF Afghanistan or a designated implementing partner, that smaller and diaspora-led providers can draw on to meet the new standards.

4. Escalate the platform-accountability track

On an ongoing basis, the Delegation should raise data-minimization and account-security features for high-risk users with EEAS Headquarters for inclusion in existing diplomatic and policy engagement with Meta and other relevant platform companies.

5. Guard against centralisation

The Delegation should ensure that any mapping, coordination, or registry exercise it commissions explicitly excludes identifying information about individual learners or teachers. Coordination should strengthen safety, not create a new single point of failure that could itself be targeted.

6. Consult Afghan stakeholders in setting the standards

The Delegation should ensure that the design of minimum standards and technical assistance under Options A and B includes structured consultation with Afghan women educators, provider organizations, and, where safe and voluntary, learners themselves — on acceptable levels of risk, preferred technologies, household and device-sharing constraints, and the kind of support they would find most useful. This positions Afghan stakeholders as policy actors in shaping the standards that will apply to them, not only as intended beneficiaries.

Implementation Timeline

0–3 months: System-level review of provider data practices commissioned and under way.

0–3 months: Minimum data-protection conditions introduced into new and renewed Delegation-managed grants; Afghan stakeholder consultation launched.

6–9 months: Technical-assistance facility operational with interested Member State missions; first providers piloting the minimum standards.

12–24 months: Standards extended across all Delegation-funded providers; platform engagement (Option C) advanced with EEAS Headquarters; independent review of implementation and update of the threat assessment in this brief.

Conclusion

For Afghan girls and women, online education remains one of the few paths left to learning. But access alone is not enough if taking part in a course creates avoidable risks for learners, teachers, or their families. The evidence reviewed for this brief does not establish a documented case in which a breached online-learning database led directly to retaliation. It does, however, show that Taliban authorities have targeted education and restricted digital access, making the exposure of learner records a credible risk that responsible programmes should not ignore. The EU should not be described as legally responsible for every data practice in Afghanistan; rather, it has a clear opportunity—and a responsibility to use its funding carefully—to reduce risks in the programmes it supports. By attaching realistic safeguards to grants, helping providers meet them, and consulting Afghan women educators on what is safe and workable, the Delegation can protect access to education without creating new barriers to it.

References

8am Media. 2026. “Knowledge Without Borders: SOLAx Makes Free Online Education Possible for Girls of Afghanistan.” February 7, 2026. https://8am.media/eng/knowledge-without-borders-solax-makes-free-online-education-possible-for-girls-of-afghanistan/

Bouachrine, Ibtissam. 2026. “U.S. Tech Companies Owe a Duty of Care to Afghan Girls Too – of a Different Kind.” Just Security. August 14, 2026. https://www.justsecurity.org/153056/tech-companies-protect-afghan-girls/

Eagle Online Academy. 2026. “Eagle Online Academy – Free Education.” https://www.eagleonlineacademy.org/

European Commission. 2023. “EU Releases €140 Million to Support the Afghan People, in Particular Women and Girls.” https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4524

European External Action Service (EEAS). 2023. “New EU Financing for Education and Learning for More Than 200,000 Primary School Children in Afghanistan.” https://www.eeas.europa.eu/delegations/afghanistan/new-eu-financing-education-and-learning-more-200000-primary-school-children-afghanistan_en

European External Action Service (EEAS). 2025. “The European Union Provides €6 Million to Support Access to Quality Education for Afghan Children with Save the Children.” September 8, 2025. https://www.eeas.europa.eu/delegations/afghanistan/european-union-provides-%E2%82%AC6-million-support%C2%A0access-quality-education-afghan-children-save-children_en

European External Action Service (EEAS). 2026. “Five Years after Kabul Takeover, EU Support for Afghan People Continues.” August 2026. https://www.eeas.europa.eu/eeas/five-years-after-kabul-takeover-eu-support-afghan-people-continues_en

European Union Agency for Asylum (EUAA). 2026. “Afghanistan: Country Focus — 4.4.4. Access to Education.” https://www.euaa.europa.eu/coi-report-afghanistan-country-focus/444-access-education

Feminist Majority Foundation. 2025. “Taliban Bans WiFi in Afghanistan, Cutting Off a Lifeline for Women and Students.” September 18, 2025.

https://feminist.org/news/taliban-bans-wifi-in-afghanistan-cutting-off-a-lifeline-for-women-and-students/

Human Rights Watch (HRW). 2025. "Taliban's Internet Ban Further Silences Afghan Women, Girls." September 30, 2025. https://www.hrw.org/news/2025/09/30/talibans-internet-ban-further-silences-afghan-women-girls

Human Rights Watch (HRW). 2026. "World Report 2026: Afghanistan." https://www.hrw.org/world-report/2026/country-chapters/afghanistan

KabulNow. 2026. "Afghan Children: Unseen Victims of the Taliban's War on Education." May 8, 2026. https://kabulnow.com/2026/05/afghan-children-talibans-victims-war-on-education/

School of Leadership, Afghanistan (SOLA). 2025. "SOLAx: Our Online Academy." https://www.sola-afghanistan.org/introducing-solax

UNESCO. 2026. "Banned from Education: A Review of the Right to Education in Afghanistan." January 16, 2026. https://www.unesco.org/en/articles/banned-education-review-right-education-afghanistan

UNESCO and UNICEF. 2026. "UNESCO and UNICEF Urge Action to Protect the Right to Education in Afghanistan." January 24, 2026. https://www.unesco.org/en/articles/unesco-and-unicef-urge-action-protect-right-education-afghanistan

UNICEF. 2020. "UNICEF Policy on Personal Data Protection." https://www.unicef.org/documents/policy-personal-data-protection

UNICEF and International Telecommunication Union (ITU). 2020. "Guidelines for Industry on Child Online Protection." https://www.unicef.org/documents/guidelines-industry-online-child-protection