

UNHCR Submission for Global Digital Compact

Connect all people to the internet, including Schools.

a) Core Principles.

UNHCR believes that forcibly displaced and stateless communities should have equitable access to digital technology and channels in line with their hosting communities and be able to use them to pursue opportunities for lifelong learning, inclusion in the digital economy, leisure, and solutions.

UNHCR acknowledges that while many initiatives are designed to support the digital inclusion of a range of communities, in many cases forcibly displaced and stateless people are left behind. Some of these initiatives take an intersectional approach, others target specific groups, however, one thing that often ties these approaches together is a focus or presumption towards digital inclusion of nationals or citizens of state, whether implied or explicit.

However, almost all states host individuals who are not citizens - including approximately 50 million people forcibly displaced abroad or stateless. When we collectively seek to further digital inclusion and connectivity for all through the Digital Compact, we must do so keeping in mind the central, transformative promise of the 2030 Agenda for Sustainable Development and its Sustainable Development Goals - to leave no one behind. UNHCR believes this is a principle that should be carried through the compact, always inclusive of forcibly displaced and stateless communities.

To deliver on this promise of digital inclusion and connectivity for all, there are essential areas of focus that require addressing. Together we must ensure that forcibly displaced and stateless communities:

- Are meaningfully integrated into national strategies and frameworks for digital inclusion and universal access and digital gender, age and disability gaps have been dramatically reduced,
- 2) Can be supported by legal and regulatory environments that allow them to register SIM Cards, get connected, and access digital financial services.



- Can access meaningful and affordable connectivity services in line with the communities that host them, both individually and at key institutions such as schools
- have access to learning environments that prepare students, and their communities, to meaningfully engage within a connected society and make informed choices,
- 5) Can safely engage in the digital economy and pursue digitally-enabled jobs and livelihoods.
- 6) have the skills available to use and contribute to the creation of not only basic but advanced digital services for whatever purpose they choose.

Finally, that forcibly displaced and stateless people, and the communities that host them, have a vital role to play and should not been seen as passive recipients of digital transformation. We must ensure their views are heard, their priorities are built in, and their skills are leveraged – so they can help drive the change their communities want to see.

b) Key Commitments pledges actions

UNHCR will continue to play an active role in dialogue and in driving forward a digital inclusion agenda in the months and years to come, in partnership with many organizations contributing to the Digital Compact Agenda.

UNHCR believe the following collective commitments will help achieve the vision and above outlined principles that will ensure that forcibly displaced and stateless communities are not left out of the connected society and wider digital transformation:

- 1) Eliminating the connectivity coverage gap in refugee-hosting areas, rolling out infrastructure and supporting its deployment as needed
- 2) Working with communities, specifically youth, to enhance digital inclusion and break down social and cultural barriers through community-based approaches.
- Implementing targeted digital inclusion interventions aimed at marginalized groups such as women and girls, the elderly or people with disabilities.
- 4) To include forcibly displaced and stateless people within government strategy, planning and budgeting across key digital inclusion and connectivity issues, ranging from broader technology access to specific sectors such as education and health.
- 5) Accelerating Private Partnerships, moving beyond traditional partnership modalities to new and innovative arrangements designed



- to strengthen digital inclusion, improve access to jobs, technology, knowledge, and guidance.
- 6) Promoting community-led approaches and local ownership of digital solutions by working with refugee-led and community-based organizations.
- Include refugee-hosting schools and communities in national and regional digital policies, planning and budgets, encouraging actors to design for the most remote communities and locations from the onset.
- 8) To provide predictable financing to support governments and partners to expand impactful digital inclusion and connectivity programming in a sustainable manner; prioritizing inclusion of a greater number of refugee-hosting communities.
- 9) To increase access to a larger number of quality digital learning materials that are aligned to national curricula, respond to local context and needs, and are available in local languages and languages of instruction.
- 10) To ensure digital awareness and protection programming is incorporated into all digital and connectivity programming, to increase understanding and agency of refugees and host communities who engage online.

Protect Data

a) Core Principles

Realising the right to privacy and protecting the personal data of refugees, internally displaced and stateless people is a fundamental part of the international legal framework for their protection. This framework applies and must be respected both offline and online.

The authorities of host States that are responsible for determining asylum claims and which process the personal data of refugees should respect the confidentiality of asylum information and closely regulate data sharing and access, particularly in relation to the authorities of countries of origin. These standards aim to prevent new risks arising for asylum seekers or their families in the host country and protect the integrity of asylum systems as well as the safety of asylum seekers' relatives or associates remaining in the country of origin. Implementing these protections and the rights of the forcibly displaced and stateless as data subjects is of growing importance in an increasingly digital world, starting with the right to information about how their personal data is processed.



Although forcibly displaced and stateless often face obstacles in getting connected, they are increasingly online, using social media platforms and accessing digital services, including humanitarian assistance. In a global survey and consultations to develop UNHCR's Digital Transformation Strategy 2022-2026, the people UNHCR serve said that they want access to more safe and robust online services and trusted protection information. UNHCR's operations are increasingly meeting this demand, using preferred channels of the people we serve, if safe and appropriate. Some host States are also bringing online capacity to asylum systems, a trend accelerated by their responses to the Covid 19 pandemic.

These new opportunities also bring new risks. Asylum seekers and refugees can be identified and tracked online, jeopardising their protection. The sharing of or access to the personal data of refugees across national borders in digital systems, including by the private sector, must respect the established principles of refugee protection, including their right to privacy.

UNHCR and other humanitarian organizations are also concerned that personal data processed for humanitarian purposes in their information systems may be subject to cyberattacks, perpetrated by a range of actors, creating additional protection risks, particularly in fragile and conflict-affected contexts. Such attacks may lead to significant risks for people UNHCR serves and jeopardises life-saving humanitarian assistance.

b) Key Commitments pledges actions

UNHCR would like to see the GDC contain a commitment from all stakeholders to respect the established principles of international law, including refugee law, relating to the protection of personal data of asylum seekers, refugees, internally displaced people, stateless people and returnees that is processed in digital systems.

The GDC should also condemn cyberattacks on digital systems used for humanitarian assistance and call on all stakeholders to work to prevent them and to increase collective cybersecurity preparedness and response.



The GDC should urge States to reflect these digital and data protection considerations in strengthening national legislative frameworks on privacy, data protection and cybersecurity, within a human rights-based approach. The private sector, including social media platforms and suppliers of digital services, such as the financial services and ICT sectors, should be encouraged to implement these principles and set up user-centric solutions for the forcibly displaced and stateless to better manage how their personal data is processed online and help avoid risks.

The GDC should highlight the importance of increasing the digital skills of the forcibly displaced and stateless, to help fulfil their rights as data subjects, make informed choices about the digital services and service providers they use and manage their digital footprint to minimise the risks that online identification and profiling can create for them.

In these ways the GDC's multistakeholder approach can contribute to protecting individuals who are potentially at heightened risk and contribute to creating a safe digital humanitarian space, rooted in international law.

UNHCR has in place policies that regulate its processing of personal data, including the data of the people it serves. They include standards for UNHCR's sharing of and access to personal data with and by its partners, as part of the delivery of humanitarian assistance and protection. They regulate UNHCR's delivery of humanitarian assistance using digital financial services and use of digital platforms and messaging technology to strengthen communication with and accountability to the people we serve. This framework has recently been strengthened by the adoption of a General Policy on Personal Data Protection and Privacy on 22 December 2022. UNHCR also has an established cybersecurity programme that aims to secure digital systems and protect people and a new Policy on Information Security which came into effect on 1 March 2023. Operations are increasingly working with communities to strengthen their skills to manage digital risks. Digital Protection is one of the five priority areas of UNHCR's Digital Transformation Strategy. UNHCR pledges to continue efforts to meet existing and emerging challenges, including by strengthening its capacity to implement these priorities at headquarters, regional and field levels.



Apply Human Rights Online

a) Core Principles

Although forcibly displaced and stateless often face obstacles in getting connected, they are increasingly connected and online, accessing digital content and services. Online access to life-saving online protection information, feedback, complaints and response mechanism can strengthen humanitarian response and accountability to affected people. Alongside these opportunities, new digital risks arise that have a profound impact the online and offline lives of the people UNHCR serves. They include the online targeting of people on the move for exploitation, such as trafficking as well as toxic online narratives and hate speech that are both a root cause of forced displacement and a protection threat to those forced to flee.

As a matter of principle, UNHCR considers that international human rights law framework applies and must be respected both offline and online by all stakeholders. This also applies to the specific international legal framework for the protection of refugees, internally displaced and stateless people. Together they will be referred to as the "relevant international legal framework".

As a starting point, the importance of avoiding discrimination by ensuring that forcibly displaced and stateless people have the opportunity to get connected should be emphasized and the role of all stakeholders in facilitating their digital inclusion should be stressed. This extends across a broad range of areas including regulation on SIM card registration, device access to mobile telecommunications infrastructure reaching remote areas where refugees are often required to reside.

In addition to the core principles cited herein, please also refer to the other parts of UNHCR's response containing specific recommendations relevant to applying human rights online, in particular, the sections on Protecting Data, Promoting the Regulation of AI and Accountability for Discrimination and Misleading Content.

UNHCR would welcome a commitment, in principle, from all GDC stakeholders to defining, maintaining and increasing "safe humanitarian digital space" based on the relevant international legal framework and international humanitarian law.



As a core principle, GDC could emphasize that the use of digital technology to control borders should facilitate access to asylum, not create new barriers to reaching safety. The opportunities increase accuracy, efficiency and integrity of asylum, family reunification and resettlement processes or strengthen protection and humanitarian response by predicting and responding to population movements stemming from conflict or natural disaster could be welcomed, whilst highlighting the importance of avoiding risks.

The strengthening of effective due diligence processes, including human rights due diligence and privacy and data protection are potentially important mechanisms for all stakeholders to realise these principles.

b) Key Commitments pledges actions

UNHCR would welcome the GDC, including commitments from all stakeholders that the relevant international legal framework applies online and offline and to respect the principles therein. Although UNHCR supports a GDC focus area on applying human rights online but noting the cross-cutting nature of this theme, these considerations should also be mainstreamed across the Compact.

UNHCR's Digital Transformation Strategy 2022-2026 contains a guiding principle on promoting protection, human rights and ethical standards in its use of digital technology and a focus area on Digital Protection that includes a set of priority actions and results that UNHCR aims to achieve. This includes increased engagement with all stakeholders and partners to promote these objectives. UNHCR pledges to continue to realise these foundational elements of its Strategy as part of a broader implementation plan, including strengthening its capacity. For example, as noted in detail elsewhere UNHCR is actively contributing the development of internal UN Guidance on Ethics and Artificial Intelligence and Human Rights Due Diligence and Digital Technologies, including piloting approaches to implementation.

Accountability for Discrimination and Misleading Content

a) Core Principles



Digital channels offer many opportunities for forcibly displaced and stateless people. But as digital platforms are incorporated into almost every aspect of our lives and societies, the potential for good is diminished by harmful online behaviours leaching from the margins of the digital ecosystem into the mainstream. There is a pervasive surge in discriminatory and misleading content such as misinformation, disinformation and hate speech. These are causing both direct and indirect real-world harm to the most vulnerable, especially refugees, displaced and stateless people, fueling xenophobia and racism, fear, suspicion and mistrust. Real-life harms include challenges in accessing protection, persecution and hate crimes, fraud and bullying, sexual exploitation and abuse, trafficking, gender-based and other forms of violence, and killings. Discriminatory and misleading content can be a factor in displacement, as seen in Myanmar where a 2018 UN fact finding mission stated that the role of social media was significant in circulating hate speech that contributed to hundreds of thousands of Rohingya being forced to flee the country.

Discriminatory and misleading content is impeding humanitarian action, especially in crisis and conflict, following natural disasters, and during election cycles, as well as protracted situations. Data shows how mis/disinformation thrives in emergency contexts where the integrity of information is vital. Coordinated inauthentic behaviour, as well as unintended misinformation, can damage reputations, erode trust and legitimacy of humanitarian organizations. It can hamper UNHCR and partners' ability to protect refugees, displaced and stateless people, threaten the physical security of humanitarian workers, and jeopardize donor support.

Digital and social media platforms have been widely institutionalized. People rely on them to be heard, to organize and to drive change. For education and livelihoods, connection with loved ones, and access to news and information. These platforms should be a safe place for all – not just people who use them in the most widely-spoken languages, live in their priority markets, and can afford subscription models to better terms of service. The protection of stateless and displaced people is increasingly threatened by attacks on information integrity. Strengthening digital protection is a priority for UNHCR and many of its UN and NGO partners, including through UNHCR's Digital Transformation Strategy 2022-2026.



b) Key Commitments pledges actions

All stakeholders should commit to making digital platforms more accountable and transparent, with safety by design and the respect for international human rights law and the international legal framework on the protection of refugees, internally displaced and stateless people at their core. Experts from diverse backgrounds and affected populations, including refugees, stateless and the internally displaced, must be meaningfully included in these efforts.

The GDC should urge the private sector to invest in diverse Trust and Safety capacities. It should emphasize the importance of human content moderation mechanisms, alongside promoting ethical and human rights use of AI, in all languages and locations their platforms are used in. In the development of search products, generative AI and other relevant technologies, the private sector should be strongly encouraged to incorporate fact-checking and other measures to minimize their risk of propagating misinformation. The GDC should call on platforms to stop profiting from harmful content, providing financial incentives for its distribution, and generating income from discriminatory and misleading advertising. The private sector should be encouraged to support independent research into links between platform architecture and misinformation. It should support UN and civil society efforts to provide credible and impartial public information by ensuring their accounts and content are accessible, verified, and not downgraded by algorithms, especially given the importance of providing information to vulnerable populations in conflict and natural disaster contexts. Governments should be encouraged to strengthen trusted channels for communications, and take measures to protect stateless and displaced populations and humanitarian personnel from discriminatory and misleading content, in full respect for international human rights law.

Civil society should be encouraged to strengthen research and mitigation efforts, seeking insights from affected populations, especially in the Global South, and empowering community-based early warning systems. Media organizations should be asked to report on the origins and impact of discriminatory and misleading content, and to strengthen standards for fact-checking organizations. Opportunities for the UN system to coordinate and convene stakeholders should be welcomed. UN entities should be encouraged to offer expertise and facilitate collaboration, including aligning design and content moderation with local needs and sensitivities.



Regulation of artificial intelligence

a) Core Principles

Rapidly emerging, high-impact technologies such as Artificial Intelligence ("AI") must be developed and used in ways which fully respect developing ethical standards and international law. This includes international human rights law, including the right to seek and enjoy asylum, and the international legal framework on the protection of refugees, internally displaced and stateless people. All has the potential to advance protection objectives and strengthen humanitarian response. The further regulation of AI is necessary to promote these objectives and manage the risks that arise.

UNHCR has actively contributed to the development of the Principles for the Ethical Use of AI in the United Nations System ("the UN AI Principles"), which are based on UNESCO's Recommendation on the Ethics of Artificial Intelligence. It is also working closely with UN Partners to develop the United Systems Guidance on Human Rights Due Diligence and Digital Technologies, under the Secretary-General's Roadmap on Digital Cooperation and Call to Action on Human Rights. These are useful reference points for all actors, including States and the Private Sector, in regulating the whole of AI System's lifecycle, which includes its "conception, design, use, development and further deployment" (see Human Rights Council Resolution on New and Emerging Digital Technologies (2021) A/HRC/47/L.12/Rev.1, para. 5).

Al regulation should play particular attention to situations where the risks of human rights violations and unethical applications are higher. This includes refugee protection, asylum, border control, as well as situations of conflict and fragility.

Al regulation must not contain exemptions or limitations that constitute or exacerbate discrimination and may negatively impact on human rights or refugee protection. This could include that some uses of Al in the areas of asylum, immigration and border control are not exempted from the full safeguards that are applied to the use of Al for other purposes.

Further research is required into the risks that can arise from the use of AI in specific contexts of particular concern to UNHCR, such as for the determination



of legal status (refugee, statelessness or nationality), including by State authorities. They present clear risks to accountability for such decisions, raise questions on proportionality and transparency and available and accessible pathways of redress for affected individuals. These risks must be addressed in a manner that is consistent with international human rights, refugee and statelessness law, with prohibitions put in place for certain uses or systems where the risk is unacceptable.

It is particularly important to ensure that AI systems are both developed and used with respect to the right to privacy and that data sets used for training must not build in discrimination or bias into AI systems, including by amplifying pre-existing societal biases.

b) Key Commitments pledges actions

UNHCR would like to see the GDC reflect the principles set out in its response to the preceding section. This includes a focus on the application and implementation of existing standards in international law and respect for ethical standards as a foundation for the regulation of AI. The GDC could explicitly call for all stakeholders, including States and the private sector, to apply those standards to the use of AI that impacts on the forcibly displaced and stateless, where higher risks are likely to apply.

UNHCR pledges to use AI in ways that are consistent with its Digital Transformation Strategy 2022-2026. This includes the Strategy's guiding principles on protection, ethics and human rights and the following specific commitments therein:

- UNHCR's conception, design, use, development and further deployment of digital technology, including AI, will meet international human rights and ethical standards, with a focus on high-risk technologies, uses and contexts.
- 2) Prioritising the further strengthening of UNHCR's capacity to apply digital technologies consistent with these principles.
- 3) By engaging and working with governments and private sector partners, UNHCR will promote full consideration of the impact of digital solutions, including AI, on the protection of the communities UNHCR serve, particularly in high-risk contexts.
- 4) UNHCR will ensure increased investment in cybersecurity and the protection of the personal data it processes, including in AI systems.



Under the Digital Protection focus area of the abovementioned Strategy, an implementation plan includes measures to realise these strategic objectives. UNHCR is currently piloting approaches to implement the UN AI Principles and the emerging United Nations System-Wide Guidance on Human Rights Due Diligence and Digital Technologies Guidance alongside new and strengthened UNHCR policies on Privacy and Protection of Personal Data (2022) and Information Security (2023). The implementation plan also envisages specific research on the uses of AI of potential concern to UNHCR under its Mandate, which are highlighted in the section above.

In addition, UNHCR's Policy on Privacy and Protection of Personal Data provides that UNHCR's use of Al will respect individuals' right to privacy and data protection, including safeguards against the risk of being subject to automated decision-making where a decision produces adverse legal or other significant adverse effects on the interests of the affected individual.

The deployment of "general purpose" AI systems in high-risk contexts such as asylum, immigration and border control, are likely to give rise to particular risks. The GDC could reference this and the increased responsibility that results for the private sector entities that develop "general purpose" AI systems.