

# UNHCR Submission for Global Digital Compact

3) Caarag (c) 25 (g) a h 0 g f u e r d 5 2 f o r d a 4 ( e d ) 1 1 s t ( 2 ) 5 0 . 5 t 2 5 5 c o r n 0 0 1 a e z , 2 i 5 ( 2 5 t ( 0 t 2 . 5 ) ) - 4 ( 2 ) s e j

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.
- 7) 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 re  
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 2026, the people UNHCR serve said that they want access to more safe and robust online services and trusted protection 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.

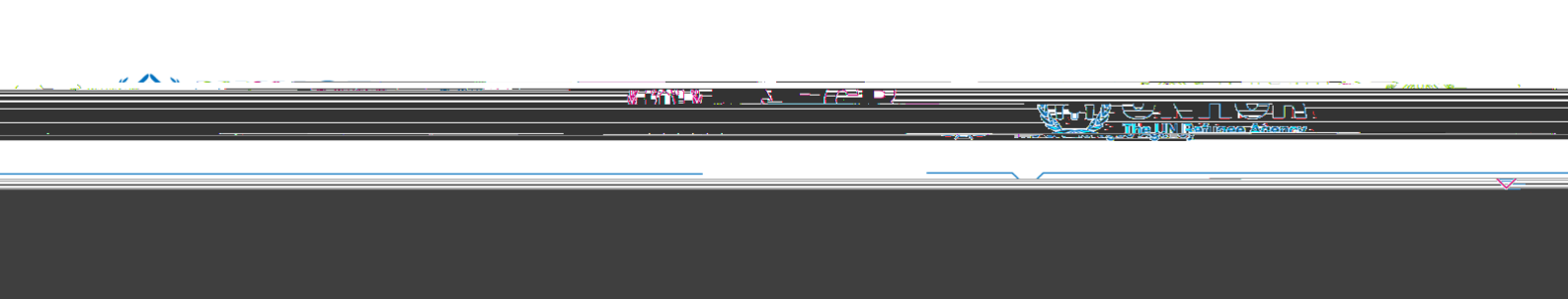
These new opportunities also bring new risks. Asylum seekers and refugees can be identified and tracked online, jeopardising their protection. The sharing of or access to the personal data of refugees across national borders in digital systems, including by the private sector, must respect the established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

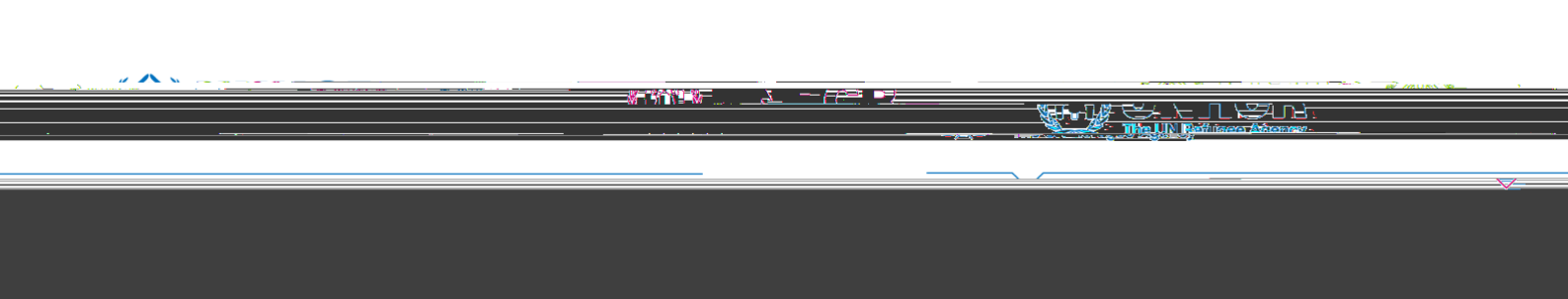
The GDC should also condemn cyberattacks on digital systems used for humanitarian assistance and call on all stakeholders to work to prevent them and to increase collective cybersecurity preparedness and response.




## Apply Human Rights Online

### a) Core Principles

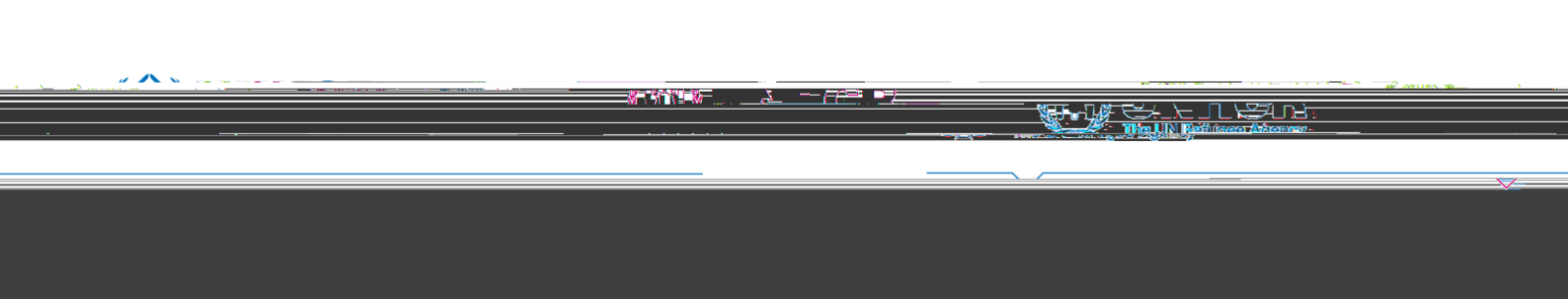
Although forcibly displaced and stateless often face obstacles in getting connected, they are increasingly connected and online, accessing digital content and services. Online access to life-saving online protection information, feedback, complaints and response mechanism can strengthen humanitarian 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  
level

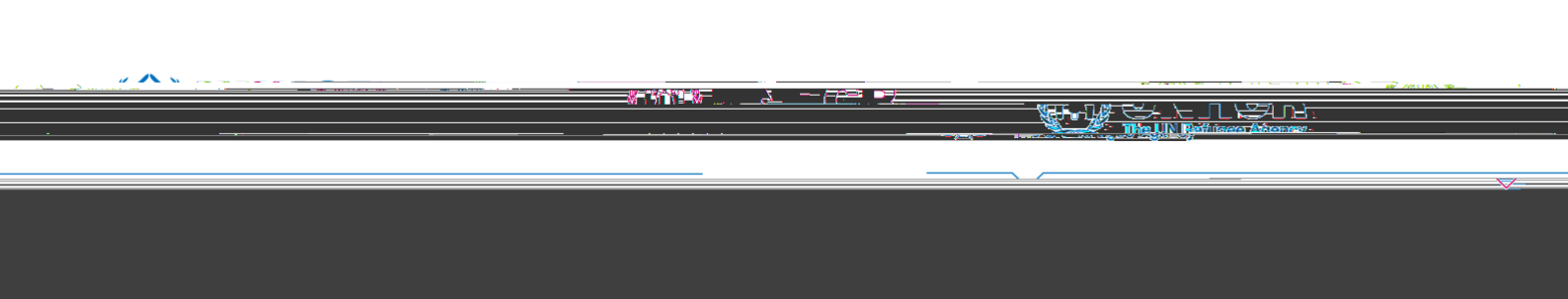


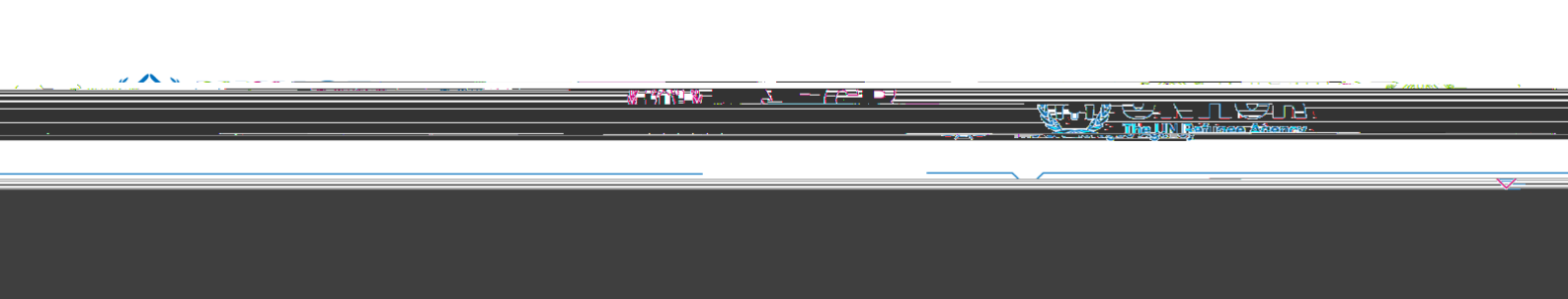


Digital channels offer many opportunities for forcibly displaced and stateless people. But as digital platforms are incorporated into almost every aspect of our lives and societies, the potential for good is diminished by harmful online behaviours leaching from the margins of the digital ecosystem into the









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 Privacy and Protection of Personal Data provides that UNHCR's AI will respect individuals' right to protection, including safeguards against the risk of being subject to automated decision-making where a decision produces adverse legal or