SUBMISSION OF INPUTS FOR THE GLOBAL DIGITAL COMPACT

April 30, 2023| India

I. Introduction

The Council for Social and Digital Development (CSDD), the Digital Empowerment Foundation (DEF), the North East Development Foundation (NEDF), and the Royal Global University (RGU), Assam, and the eNorth East Digital Alliance, is pleased to submit inputs to the Global Digital Compact (GDC). The inputs are based on a stakeholder's discussion from the North East Region of India in South Asia (comprising of 8 States covering the North East India Himalayan States), through online mode (Zoom meeting) on April 28, 2023. The discussion was on the state of connectivity and the social aspect to digital access and technological advancements with a focus on north east Indian states, the geographical spread of which greatly overlaps with the eastern Himalayan region.

II. Description of entity/organization

The Council for Social and Digital Development (CSDD) is a research and policy advocacy organization working at the intersection of technology and society. Based out of Guwahati, Assam in the north east region of India, the council works towards evidence building, creating narratives, building narratives on emerging digital and society related issues in the particular context of North East India, a predominantly tribal region.

III. KEY AREAS / CORE PRINCIPLES / KEY COMMITMENTS

1. Connect all people to the Internet, including all schools

Core Principles

- **Structured, systematic and process-oriented Internet Access:** The COVID-19 pandemic hastened the adoption of internet for all including amongst the school-going children. There needs to be a structure way the internet is adopted in schools and by the young learners as well as the educators / teachers. There should be sensitisation of the teachers and instructors to help guide the young, impressionable children on what the internet can offer.
- **Need and Capacity Oriented Access:** Internet is one of the great levelers in helping bridge the information gap. But there needs to be evaluation of needs of an institute when providing internet. What are they going to deliver to the students? Where are they going to create? Where are they going to store what they create?
- **Content as Core:** Initiatives in the education and other sector with regards to internet is without any content management. In the absence of quality content delivery, incongruence between demand and delivery of content, asymmetry between the subject and course delivery, then mere connectivity is fruitless. Education and specific content delivery digitally must have content charter that outlines and provides guidance on what, how, when to deliver content to consumers and learners in schools.
- **Asymmetric connectivity**: The geographical and topographical internet and access divides can be addressed with heavy focus on robust satellite connectivity for the inaccessible regions as the traditional modes of mobile phone tower and fiber cable connectivity face additional challenges of maintenance in the regions due to the geographic terrain. There is need to explore alternative networks and portable networks to help connect people living in difficult terrains with bad network connectivity.
- **'Integrated Connectivity'**: Besides rural and remote geographies, even in semi urban areas connectivity is a big challenge, and rural connectivity has a long way to

go. It is not internet alone but all the supporting infrastructure of regular electricity supply, last mile networks, access to devices needs to work in congruence as an integrated toolkit.

- **Satellite Connectivity as a key priority:** Cost of accessing internet connectivity will come down in the next few years with the proliferation of satellite connectivity. But reliance on physical infrastructure like towers, fiber is going to be counterproductive.
- **Meaningful connectivity and affordable connectivity**: should be guiding factors to make 'Internet for all' a real possibility. This has larger inclusive and sustainability significance.
- **Internet and digital training** must be a core component in connectivity and access for all. Training of the trainers or of teachers and instructors to efficiently guide students to build competencies and make meaningful use of internet. The generational internet and digital gaps need emphasis on internet and digital skills training.
- **The 'Quality of bandwidth' determines 'Quality of Life':** Quality of bandwidth being delivered to people and classrooms needs to be analysed and optimised to be truly useful instead of focusing only on connecting to the internet.
- **'Public Internet Access':** Policies and programmes must be designed and sustained for more public open spaces with open and free Wifi connectivity. Low cost public Wifi zones should be intensified. The millions of unconnected people need special arrangements like Community Internet Libraries (CILs) to mainstream people in remote community. Efforts like this can stop incidences of Net micro-migration in villages where people are migrating to areas where they can get access to internet connectivity during times of examinations, as was evident in the peak of the pandemics.

Key Commitments from Stakeholders

- **Infrastructure investment:** To guarantee that everyone has access to the internet, governments should invest in developing the required infrastructure, such as broadband networks. Public-private partnerships or initiatives supported by the government can be used to accomplish this.

- **Promoting digital literacy:** To make sure that everyone has the skills and information required to use the internet efficiently and safely, civil society organisations, governments, and businesses should encourage digital literacy programmes.
- **Accessibility:** Businesses and governments should endeavour to ensure that everyone has inexpensive access to the internet, especially those who live in rural or low-income areas.
- **Ensuring user privacy and security:** When connecting consumers to the internet, governments and businesses should prioritise their privacy and security. This can be accomplished by rules, guidelines, and instruction on safe internet usage.
- **Fostering innovation:** To broaden access to the internet and enhance its capabilities, businesses and governments should support innovation and the creation of new technologies.
- **Collaboration with stakeholders:** To accomplish the aim of universal internet access, all stakeholders—including schools—should cooperate and work together. Partnerships between governments, businesses, and groups from civil society are examples of this, as well as interactions with nearby communities and educational institutions to learn about their wants and requirements.

2. Digital commons as a global public good

Core principles

The following are some of the core principles for digital commons as a public good:

- **Accessibility:** Digital commons should be easily accessible to everyone, regardless of their background, income, or social status. This includes access to digital infrastructure, tools, and services that enable people to participate in the digital commons.

- **Openness:** Digital commons should be open and transparent, allowing for free access, use, and modification of the digital resources. This includes open data, open-source software, and open educational resources.
- **Collaboration:** Digital commons should be based on collaborative and participatory models of production, where individuals and communities work together to create and maintain shared digital resources.
- **Sustainability:** Digital commons should be sustainable over the long term, with a focus on maintaining and improving the quality of the digital resources for the benefit of current and future generations.
- **Diversity:** Digital commons should be diverse and inclusive, reflecting the needs and perspectives of different communities and cultures. This includes promoting cultural diversity, linguistic diversity, and gender diversity.
- **Privacy and security:** Digital commons should be designed with strong privacy and security measures to protect users' personal data and prevent unauthorized access or misuse of digital resources.
- **Democratic governance:** Digital commons should be governed in a democratic and transparent manner, with clear and fair rules for decision-making, participation, and accountability.

Key commitments

- **Transparency:** Institutions, businesses, and other parties involved in decision-making must pledge to be transparent in their operations. This covers open standards, open-source software, and open information access.
- **Collaboration:** To make digital commons a public good, collaboration is essential. To do this, governments, businesses, civil society organisations, and other interested parties should cooperate and pool their knowledge, resources, and skills.
- **Accessibility:** Regardless of a person's geographic location, socioeconomic level, or other circumstances, digital commons must be available to all. Governments and other interested parties ought to pledge to make sure that everyone has access to and participation in the digital commons.

- **Privacy and Security:** Governments, companies, and other stakeholders must commit to ensuring the privacy and security of digital commons. This includes protecting personal data and ensuring that digital commons are secure from cyber-attacks.
- **Sustainability:** Digital commons must be sustainable over the long term. Governments, companies, and other stakeholders should commit to ensuring the long-term sustainability of digital commons by investing in infrastructure, capacity building, and other initiatives.
- **User Empowerment:** Users must be empowered to participate in the creation, management, and governance of digital commons. Governments, companies, and other stakeholders should commit to providing users with the tools, resources, and support they need to participate in digital commons.
- **Public Benefit:** Digital commons must serve the public interest, rather than private interests. Governments, companies, and other stakeholders should commit to ensuring that digital commons are designed and managed to serve the public good, and that the benefits of digital commons are distributed equitably.

3. Avoid internet fragmentation

Core principles

- Internet must remain interoperable and interconnection across all regions must be assured to allow democratic access.
- Internet fragmentation leads to security vulnerabilities
- Principles of net neutrality should be adhered to put a check to internet fragmentation.

Key commitments

- Multi-stakeholder governance of the internet should be made actionable.
- Internet fragmentation due to commercial consideration needs to be addressed better.

- Governments should refrain from making digital sovereignty decisions which lead to internet fragmentation.

4. Promote regulation of artificial intelligence

Core principles

- **Transparency:** AI systems should be designed and developed in a transparent manner so that users and stakeholders can understand how the system works and make informed decisions about its use.
- **Accountability:** Developers, users, and other stakeholders should be held accountable for the impact of AI systems on individuals, society, and the environment.
- **Fairness:** AI systems should be designed and developed in a way that is fair to all individuals and groups, regardless of their race, gender, religion, or other characteristics.
- **Safety and security:** AI systems should be safe and secure, and designed to minimize the risk of harm to individuals and society.
- **Privacy:** AI systems should be designed and developed in a way that respects individual privacy and data protection.
- **Human-centered design:** AI systems should be designed to enhance human capabilities and support human well-being.
- **Ethical considerations:** Developers and other stakeholders should consider the ethical implications of AI systems, including issues related to bias, discrimination, and human dignity.
- **Data Justice:** AI based data processing; usage should be based on ‘data justice’ principles.

Key commitments

Government:

a) Develop and implement clear policies and regulations that guide the development and deployment of AI technologies.
b) Establish a framework for ethical considerations in AI development and use.
c) Foster collaboration between government, industry, academia, and civil society to ensure that the benefits and risks of AI are adequately assessed and addressed.
d) Encourage transparency and accountability in the development and deployment of AI technologies.
e) Invest in research and development to ensure that AI technologies are developed in a way that benefits society as a whole.

Companies:

a) Develop and implement clear policies and guidelines for the development and deployment of AI technologies.
b) Foster transparency and accountability in the development and deployment of AI technologies.
c) Develop ethical frameworks for AI development and use.
d) Invest in research and development to ensure that AI technologies are developed in a way that benefits society as a whole.
e) Ensure that AI technologies are designed to be fair and unbiased, and do not perpetuate discrimination or inequality.

Developers:

a) Develop AI technologies in a way that is transparent, ethical, and accountable.
b) Ensure that AI technologies are designed to be fair and unbiased, and do not perpetuate discrimination or inequality.
c) Conduct rigorous testing and evaluation of AI technologies to ensure that they are safe, reliable, and effective.

d) Foster collaboration with other stakeholders to ensure that the benefits and risks of AI are adequately assessed and addressed.
e) Encourage transparency and accountability in the development and deployment of AI technologies.

Research Agencies:

a) Conduct research on the societal and ethical implications of AI technologies.
b) Develop and promote standards for the development and deployment of AI technologies.
c) Foster collaboration between researchers, industry, and civil society to ensure that the benefits and risks of AI are adequately assessed and addressed.
d) Conduct independent evaluations of AI technologies to ensure that they are safe, reliable, and effective.
e) Develop and promote ethical guidelines and a framework for the development of AI technologies.

Civil Society:

a) Advocate for transparency, accountability, and ethical considerations in the development and deployment of AI technologies.
b) Monitor and evaluate the use of AI technologies to ensure that they are fair and do not perpetuate discrimination or inequality.
c) Foster collaboration with other stakeholders to ensure that the benefits and risks of AI are adequately assessed and addressed.
d) Promote public awareness and education on the societal and ethical implications of AI technologies.
e) Encourage the development and use of AI technologies that benefit society as a whole.

5. Protect data

Core Principles

- **Consent:** Before their personal information is gathered, processed, or shared, citizens should have the freedom to manage it and provide their explicit consent.
- **Transparency:** Organisations should be open and upfront about how they gather, utilise, and share the personal information of citizens.
- **Purpose limitation:** Personal information should only be gathered and used for particular, transparently stated objectives that have been made known to the public.
- **Data minimization:** Organisations should only gather and use the bare minimum of data required to fulfil the stated objectives.
- **Security:** To prevent unauthorised access, disclosure, or destruction of citizen data, organisations should put in place the proper organisational and technical safeguards.
- **Accuracy:** Individuals should have the right to access and update any personal information that organisations may have about them.
- **Limitation on retention:** Personal information should only be maintained for as long as is required to fulfil the stated purposes.
- **Accountability:** Businesses must take responsibility for adhering to data protection laws and must be open about their attempts to do so.

Key Commitments

- **Transparent regulations and policies:** Governments should implement legislation and policies that are crystal clear in regards to data privacy and security, stating what is permitted and what is not, as well as how data breaches will be handled.
- **Robust Data Protection Laws:** Governments should pass strong data protection laws that create regulatory frameworks for privacy and data protection. Regulating agencies should enforce these laws.

- **Transparency:** Businesses should be open and honest about how they gather, store, and use data. They should give people access to their own data and be transparent about the data they acquire, how they use it, and what they do with it.
- **Consent:** Before collecting or processing a person's personal information, businesses should get that person's express consent. This consent must be freely given, precise, well-informed, and clear.
- **Data security:** To prevent unauthorised access to data, businesses should put strong data security procedures in place. They ought to create access controls, encrypt important data, and periodically assess their security procedures.
- **Data minimization:** Businesses should only gather and use the data required for the services they offer. They should refrain from gathering superfluous data and remove it once it is no longer required.
- **Accountability:** Parties responsible for data breaches or misuse should be held to account, including businesses, governments, and other entities. They should be obligated to take immediate action to mitigate any harm caused by breaches and promptly report them.
- **Education:** Governments, businesses, and civil society organisations should collaborate to educate people about data privacy and security and equip them with the tools they need to do so.
- **Collaboration:** Governments, companies, civil society, and other organizations should collaborate to develop and implement effective data privacy and security policies and practices.

6. Apply human rights online

Core Principles

- **Respect for the rule of law:** All stakeholders should respect the rule of law and ensure that human rights are protected and upheld online in the same way they are in the offline world.

- **Accessibility:** Stakeholders should ensure that everyone has equal access to the internet and digital technologies, regardless of their background, socioeconomic status, or geographical location.
- **Privacy:** All stakeholders should respect and protect individuals' right to privacy online, including their personal information and data.
- **Freedom of expression:** Stakeholders should protect and promote freedom of expression online, while also addressing any harmful content or behavior that may threaten this right. Policy should define the severity of an expression online.
- **Digital literacy:** Stakeholders should promote digital literacy and education to help people understand their rights and responsibilities online, including how to protect themselves and others from online harm. Self-regulation is equally important as part of this literacy.
- **Non-discrimination:** All stakeholders should ensure that people are not discriminated against online based on their race, gender, sexual orientation, religion, or any other characteristic.
- **Transparency and accountability:** Stakeholders should be transparent about their actions and decisions related to online human rights and be accountable for any violations that occur.

Key Commitments

- **Protecting the right to privacy:** Governments and companies must ensure that individuals have the right to control their personal data and information, and that their privacy is respected.
- **Protecting freedom of expression:** Governments must ensure that individuals have the right to express themselves freely online without fear of censorship or retaliation.
- **Ensuring access to information:** Governments and companies must ensure that individuals have access to information that is necessary for them to participate fully in society, such as news, education, and health information.
- **Preventing online harassment and abuse:** Governments, companies, and civil society must work together to prevent online harassment and abuse, and to hold

perpetrators accountable. New techs can be leveraged to identify violation of basic access to expressing opinions online.

- **Protecting against discrimination:** Governments and companies must ensure that individuals are not discriminated against online based on their race, gender, sexual orientation, religion, or any other characteristic.
- **Ensuring digital security:** Governments and companies must ensure that individuals are protected against cyber threats and that their personal data is secure.
- **Promoting digital inclusion:** Governments and companies must work together to ensure that all individuals have access to the internet and the digital tools they need to participate fully in society.
- **Holding stakeholders accountable:** Governments must ensure that companies, regulators, civil society, and other stakeholders are held accountable for their actions online and that appropriate measures are taken to address any violations of human rights.

7. Introduce accountability criteria for discrimination and misleading content

Core principles

- **Accuracy:** Any information shared online needs to be true and based on reputable sources. The information provided shouldn't be purposefully misleading or exclude vital details that would paint a fuller picture.
- **Transparency:** Content producers should be open and honest about their goals and connections. Any conflicts of interest or prejudices that might skew their reporting ought to be disclosed.
- **Responsibility:** Online content authors and publishers are responsible for the data they publish. This entails accepting responsibility for any damage the content may have caused and making an effort to redress inaccurate information or deceptive claims.

- **Respect for diversity:** Online material should respect diversity by not discriminating against or marginalising people or groups based on their ethnicity, gender, religion, sexual orientation, or handicap.
- **Ethical standards:** Creators and publishers of online content should adhere to ethical standards for journalism and communication. This includes respecting privacy, avoiding sensationalism or clickbait, and avoiding plagiarism.

Key commitments

- **Commitment to Transparency:** All stakeholders, including content creators, publishers, and platforms, should commit to transparency about their content creation and distribution processes. They should clearly state their policies on what constitutes misleading or discriminatory content and how they plan to enforce these policies.
- **Promoting Education and awareness:** All stakeholders should work to educate themselves and others about the harms of misleading and discriminatory content. This includes training content creators, publishers, and platforms on how to recognize and address such content, as well as educating the public on how to identify and report misleading or discriminatory content.
- **Ensuring Enforceability:** All stakeholders should commit to enforcing their policies on misleading and discriminatory content. This includes taking action against content creators and publishers who violate these policies, such as removing their content from platforms and holding them accountable for any harm caused.
- **Commitment for Collaboration:** All stakeholders should work together to address the problem of misleading and discriminatory content. This includes sharing best practices, collaborating on research, and developing tools and technologies that can help identify and remove such content.
- **Willingness and capacity for Continuous improvement:** All stakeholders should commit to continuously improving their policies and practices around misleading and discriminatory content. This includes regularly reviewing and updating their policies to reflect changes in the media landscape, as well as investing in research and development to identify new ways to address the problem.

Stakeholders Discussion Panel Members

1. Atreyee Borooah Thekedath, Founder CEO, Webcom (India) Pvt Ltd
2. Dr. Bhogtoram Mawroh, Senior Associate, Research and Knowledge Management, North East Slow Food and Agrobiodiversity Society (NESFAS)
3. Dr Anupam Das, Associate Professor & Co-ordinator, RSIT
4. Dr Ishita Chakraborty, & Associate Professor & Co-ordinator, RSET
5. Dr Aruna Dev Rroy, Associate Professor, RSC
6. Jayanta Deka, Digital Editor, The News Mill
7. Dr. Kaberi Bezbarua, Assistant Professor, Accountancy, Gauhati Commerce College
8. Karma M. Bhutia, Founder, Demi Solutions
9. Ninglun Hanghal, Freelance Journalist based in Imphal, Manipur
10. Sanjib Sarmah, OSD, Assam Electronics Development Corporation Limited (AMTRON)
11. Sanjeev Sarma, Founder Director & CEO, Webx Technologies
12. Dr. Syed S. Kazi, Director, Council for Social and Digital Development
13. Dr. Y. Jayanta Singh, Executive Director, National Institute of Electronics & Inf Tech. (NIELIT), AFC Building, Paltan Bazar, Guwahati - 781008, Assam

****