

China IGF Input to the Global Digital Compact

To respond to the call of contributing to the Summit of the Future and the Global Digital Compact (GDC), the China IGF delivered an open proposal to invite the Chinese Internet community to join the GDC-related consultation process and contribute input from different expertise. The community actively joined the process and shared their knowledge and insights to input as follows.

● **Connect all people to the internet, including all schools**

Core Principle 1:

The innovation and development of digital infrastructure should be promoted equitably and fairly for all.

Key Commitments:

Within international and regional cooperation mechanisms, multilateral and multi-stakeholder cooperation on digital infrastructure should be promoted through initiatives on digital cooperation as well as other means. Supports to the developing countries on Internet infrastructure construction should be encouraged. The deployment of IPv6 should be accelerated to connect more people and devices to the Internet.

Core Principle 2:

Language should not be a disincentive for people to connect to the Internet.

Key Commitments:

Internationalized Domain Names, as easy access to the Internet in native languages for people around the world, should be further deployed and implemented for Universal Acceptance.

Core Principle 3:

The development of digital technology should be inclusive, while barriers to the

application should be removed. Digital education should be strengthened.

Key Commitments:

Investment in digital education should be encouraged and supported, with domestic policies developed to enhance education and training at all levels of digital literacy. Attention should be paid to the equal rights of women, children, persons with disabilities, refugees and persons with specific needs to digital technology, and joint efforts should be made to solve their difficulties in digital technology application, so as to achieve digital inclusion.

(**Authors:** Xiao ZHANG, Lang WANG, Feng GUO, Xiaomin YANG, Rui ZHONG, Jiali LI)

● **Avoid Internet fragmentation**

Core Principle 1:

To prevent countries from imposing arbitrary restrictions on cross-border data flows and fragmenting the digital governance, based on data security rules.

Key Commitments:

Rules should be established to ensure legitimate and controllable flow of data globally, while promoting free flow.

It is essential to establish a framework rule for global regulatory compatibility of cross-border data flows. Each legal order should seek a "common law" for cross-border data flows, applying common solutions or principles to the same legal problems. Countries' domestic legislation should interact with the international rule of law, and the domestic data security regulatory system should align with national security exceptions to guide, encourage and promote cross-border data flow. This is essential to suppress the prohibitions in domestic data security laws and eliminate the arbitrariness of applying national security exceptions that restrict cross-border data flow.

Core Principle 2:

Ensure the integrity and reliability of Internet infrastructure and core resources.

Key Commitments:

Protect Internet infrastructure, support its construction, maintain the neutrality of Internet core resources, and maintain the commonality of digital access technologies. A consensus-based system should be built for research and knowledge sharing on network fragmentation. It is essential to enhance resilience and elasticity to respond to the impact of network fragmentation with a focus on technical standards, industrial ecology, and global supply chains. Critical infrastructure supporting the global network should be protected effectively.

Core Principle 3:

Support a sustainable technology community.

Key Commitments:

It is essential to maintaining technical community development sustainability, enhancing trust among technical community members, improving knowledge sharing levels, and strengthening the ability of technical communities to deal with threats. It is necessary to promote the construction of a technical community governance community.

(**Authors:** Xingdong FANG, Wenxiang ZHANG, Yilin SUN, Yi SHEN, Xiangming ZHONG)

● Protect Data**Core principle 1: Guarantee data security****Key commitments:**

The security of critical information infrastructure and application design should be ensured. Measures such as data encryption should be taken to guarantee data security. The adoption of data classification system should be considered, and a balance between

data security and data development should be struck. Attention should be paid to the accuracy, high-quality and standardization of data. Data integration and interoperability should be improved.

Core principle 2: Protect personal data and privacy

Key commitments:

The legislation should endow individuals with rights to their personal data, preventing and stopping infringement of personal data rights. Personal data processing should uphold the principles of lawfulness, legitimacy, necessity, and good faith. The collection of personal data should not be excessive and illegal, and should be limited to the minimum scope for the purpose of processing. The period for storing personal data should not exceed the necessary period stipulated by law.

Core Principle 3: Maintain data fairness and justice

Key commitments:

The principle of universality and inclusiveness of data should be upheld, and data bias, marginalization, and discrimination should be avoided. Digital literacy education and digital capacity building are important countermeasures in bridging data divide, knowledge gap, etc. Individuals and organizations should be given equal access to and can benefit equally from data, information, and knowledge with public interest attributes.

Core Principle 4: Guarantee the responsibility and accountability of relevant actors

Key commitments:

Data should be developed and utilized in accordance with laws, regulations, and ethical principles. Accountability mechanism should be included in data protection laws and regulations and full implementation should be achieved.

Core Principle 5: Adhere to multi-party data governance

Key commitments:

All parties should work together to enhance the utilization, development, and security of data. Institutional and law enforcement capabilities should be strengthened. The improvement of data protection abilities is indispensable for the public, and the supervision of data protection is also a necessity.

Core Principle 6: Enhance international cooperation and mutual trust in data

Key commitments:

International cooperation in data security governance, data development and utilization should be strengthened, promoting the orderly and free cross-border data flow according to laws. Mutual trust in data security and ICT utilization should be enhanced. The formulation of global rules should be promoted under the framework of the United Nations, and the global rules of cross-border data flow should leave adequate policy space.

(**Authors:** Yongjiang XIE, Xuefeng ZHOU, Yik Chan CHIN, Xingdong FANG, Yunfei ZHOU, Xiaonan LI, Na LI, Lei WANG, and Xiaobo YANG as rapporteur)

● **Apply human rights online**

Core Principle 1:

Ensure the connectivity, resilience, and security of the Internet's critical infrastructure and resources.

Key commitments:

Recognize the Internet's critical infrastructure and key resources as the public core in international law or international code of conduct.

Core Principle 2:

Establish an environment for inclusive and equal participation in the development of

Internet technical standards, regulatory mechanisms and frameworks.

Key commitments:

Establish inclusive and equitable environments, participatory mechanisms, and capacity-building programs such as skills and knowledge trainings and funding to encourage and support various vulnerable groups such as women, the elderly, people with disabilities, to effectively and equally participate in Internet governance.

Core Principle 3: Emphasize the indivisibility of all human rights, systematically and comprehensively promote economic, political, social, cultural, environmental rights in digital sphere.

Key commitments:

Uphold the international legal system and the spirit of international law with the UN Charter at its core, reaffirm the indivisibility and balance in the human rights legal system, and the balance with other legal regimes, and establish a sound legal support system to ensure that all people can enjoy the accessibility, security and benefits of the Internet.

Core Principle 4:

Build a more interactive and inclusive participatory governance system, improving international cooperation and strategic engagement with other players and forums of governance systems at global and regional levels.

Key commitments:

Encourage multi-stakeholders to actively promote the construction and improvement of a participatory governance system; establish an inclusive and open governance system, participation mechanism and capacity building plans; establish an expert pool of governance participants, and encourage global and regional international cooperation and strategic engagement of stakeholders.

Core Principle 5:

Digital Inclusion

Key commitments:

Develop a technology transfer plan from developed to less developed countries/communities.

(Authors: Yi SHEN, Yik Chan CHIN, Peixi XU, Yilin SUN)

● **Introduce accountability criteria for discrimination and misleading content**

Core Principle 1:

Any propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

Key Commitments:

States should be prohibited from using information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability. States should cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds. Private sector should incorporate the key principles against war propaganda and national, racial or religious hatred into its terms of use or community rules and have them implemented in content moderation. Civil society organizations, technical community, and academia as well should work together to ensure that the notification, criteria, and remedy mechanism regarding discrimination and misleading content work properly and impartially.

Core Principle 2:

Maintain a principle of inclusion and responsibility.

Key Commitments:

Social media platforms should embrace diversities and be independent of politics, races, ethnic groups, religions, and gender as well. Social media platforms should establish mechanisms, criteria, and procedures of dispute resolution regarding discrimination and misleading content. Professional and traditional media also play a key role in eliminating discrimination and misleading content by following certain news norms.

Core Principle 3:

Follow a principle of enhancing digital literacy education.

Key Commitments:

Efforts should be taken to enhance digital literacy education to ensure that citizens have a critical attitude towards the information or content they encounter, to help recognize discrimination and misleading content, and improve the degree of democratic participation. Digital literacy education can help vulnerable individuals and groups to improve their awareness of online risks. Different measures can be directed to different population groups such as the youth and the old for their specific needs and risks. Digital literacy courses should include those that can help children improve their digital skills and avoid harms of discrimination and misleading content. Meanwhile, necessary training resources should be prepared to improve the digital literacy of parents, other supervisors or teachers.

(**Authors:** Peixi XU, Yongjiang Xie, Xuefeng ZHOU, Yi SHEN)

● **Promote regulation of artificial intelligence**

Core Principle 1: Inclusiveness

The principle of inclusiveness contains five dimensions: social well-being, fairness and

justice, diversity, balance, and sustainability.

Core Principle 2: Safety and Security

The principle of safety and security contains four dimensions: reliability, controllability, traceability, and accountability.

Core Principle 3: Cooperation

The principle of cooperation contains three dimensions: openness, credibility, and equality.

Core Principle 4: Agility

The principle of agility contains three dimensions: dialogue, mutual-reference, and interoperability.

Key Commitments:

The following action plans are proposed to implement the principles of AI development and governance effectively.

1. Establishing an International Cooperation Platform for AI Development and Governance

Establish and maintain an international cooperation platform for AI development and governance under the United Nations system to strengthen international cooperation.

The platform could be similar to Internet Governance Forum, and aims at promoting value consensus, standard formulation, rule negotiation, and experience sharing, etc.

2. Constructing an Evaluation System for AI Development and Governance

Stick to the philosophy of "ethics pioneering the way forward", all nations should actively explore and establish AI ethical impact assessment frameworks to develop the practical guides of AI ethics, formulate the audit and administrative rules on engineering ethics, innovate the designation of rules and tools, and enhance the capacities building of AI security evaluation and control. Encourage the transnational sharing of best practices, and conduct international dialogues and form international

consensus.

3. Initiating an Education Program for AI Ethics and Digital Literacy

Launch the "AI Education Popularization Program" to reduce digital inequality caused by the widespread adoption of AI, and enhance the capacity of disadvantaged, vulnerable groups, and minority groups to apply AI. Launch the "AI Ethics Education and Training Program" to improve the ethical level of practitioners and promote the development and application of AI in a responsible and ethical manner.

(**Authors:** Yilin SUN, Yan LI, Xuefeng ZHOU, Jing ZHAO, Yi SHEN, Ying CHEN, Xiaonan LI, Kai JIA)

Note: Where any discrepancy arises between the English translation and the Original Chinese version (Appendix 2), the Chinese version shall prevail.

Appendix 1:

Coordinators:

- Chengqing HUANG, Vice President, Chair of China IGF, Vice President of the Internet Society of China (ISC)
- Xiao ZHANG: Executive Vice Chair of China IGF, Deputy Director General of the China Internet Network Information Center (CNNIC)
- Rui ZHONG: Secretary General of China IGF, Director of International Affairs Department, ISC

Authors:

- Xiao ZHANG: Executive Vice Chair of China IGF, Deputy Director General of CNNIC
- Lang WANG: Vice Chair of ICANN GAC, Head of International Affairs Department of CNNIC
- Feng GUO: Deputy Secretary General of China IGF, Policy Researcher of the China Academy of Information and Communications Technology (CAICT)
- Xiaomin YANG: Policy Researcher of the CAICT
- Rui ZHONG: Secretary General of China IGF, Director of International Affairs Department, ISC
- Jiali LI: Project Manager, International Affairs Department of ISC
- Xingdong FANG: Qiushi Distinguished Professor, Zhejiang University; Director, Wuzhen Institute for Digital Civilization
- Wenxiang ZHANG: Professor, School of Cyber Science and Technology, Zhejiang University
- Xiangming ZHONG: Secretary General, Consortium of Internet and Society, Communication University of Zhejiang
- Yilin SUN: Deputy Secretary General, Senior Engineer, Institute of International and Strategic Studies, Peking University
- Yi SHEN: Professor, School of International Politics and Public Affairs, Fudan University

- Yik Chan CHIN: Associate Professor, School of Journalism and Communication, Beijing Normal University
- Peixi XU, Professor, the Communication University of China
- Yongjiang XIE, Professor, School of Cyberspace Security, Beijing University of Posts and Telecommunications
- Xuefeng ZHOU, Vice Dean & Professor, Law School of Beihang University
- Yunfei ZHOU, Intern, Division for Public Institutions and Digital Government, United Nations Department of Economic and Social Affairs
- Xiaonan LI, Assistant Professor, Law School, Zhengzhou University
- Na LI, Policy Researcher, Internet Governance Research Center, Fuxi Institution
- Lei WANG, Researcher, Lab for AI & Law, Beijing Institute of Technology
- Xiaobo YANG, Director of Internet Governance Research Center, Fuxi Institution
- Yan LI, Director of Institute of Sci-tech and Cybersecurity, China Institute of Contemporary International Relations
- Jing ZHAO, Associate Professor, School of Public Policy and Management, Tsinghua University
- Ying CHEN, PhD Candidate, School of Public Policy and Management, Tsinghua University
- Kai JIA, Associate Professor, University of Electronic Science and Technology of China

Appendix 2:

中国 IGF 关于“全球数字契约”的建言

一、关于数字连接

(Connect all people to the internet, including all schools)

核心原则 1: 公平促进数字基础设施建设与创新发展。

关键承诺:

在全球和地区组织及合作机制内，通过发布数字合作倡议等方式，推动多边与多方加强数字基础设施合作；鼓励向发展中国家提供数字基础设施建设支持；支持 IPv6 加快部署，以连接更多的人和设备上网。

核心原则 2: 语言不应成为人们连接互联网的阻碍因素。

关键承诺:

国际化域名应当进一步部署和实施，促进普遍接受，以方便全球各地的人使用母语上网。

核心原则 3: 支持数字技术包容发展，消除数字应用壁垒，强化数字教育。

关键承诺:

鼓励支持对数字教育的投入，在本国推动制定相关政策

加强数字素养和技能面的教育与培训。重视妇女、老人、儿童、残疾人、难民和有具体需求人士享受数字技术平等权利问题，共同推动解决其在运用数字技术方面遇到的困难，实现数字包容发展。

二、关于避免互联网碎片化

(Avoid internet fragmentation)

核心原则 1：防止各国基于数据安全规则对数据跨境流动限制的随意性和数字治理的碎片化。

关键承诺：

构建数据跨境流动正当可控规则，促进全球数据自由流动的同时，保证数据大规模流动和利用过程的正当性和可控性。

建立数据跨境流动全球规制兼容性框架规则，各法律秩序寻求数据跨境流动的“共同法”，相同的法律问题能适用共同的解决方案或共同原则。各国国内立法与国际法治互动，国内数据安全规范体系与国家安全例外条款对接，引导、鼓励和促进数据跨境流动，从而达到压制国内数据安全法中的禁止性规定，以实现破除国家安全例外条款在限制数据跨境流动中适用的随意性之效果。

核心原则 2：确保互联网基础设施和核心资源的完整性和可

靠性。

关键承诺：

保护互联网基础设施；支持互联网基础设施的建设；保持互联网核心资源的中立性；保持数字接入技术的通用性；构建基于共识的网络碎片化研究与知识共享体系；以技术标准，产业生态和全球供应链为侧重点，提升应对网络碎片化冲击的韧性与弹性；有效保护支撑全球网络的关键基础设施。

核心原则 3：支持可持续发展的技术社区。

关键承诺：

保持技术社区发展的可持续性；维护与增进技术社区成员间的信任；提升技术社区的知识共享水平和应对威胁的能力；推进技术社区治理共同体的构建。

三、关于数据保护

(Protect data)

核心原则 1：确保数据安全。

关键承诺：

保护关键信息基础设施安全。确保应用设计安全性，采取加密等措施保障数据安全。采取分类分级的数据保护思路，兼顾安全与发展平衡。重视数据的准确性、高质量性和标准化，促进数据整合互通和互操作。

核心原则 2： 保护个人数据和隐私。

关键承诺：

通过立法赋予个人对其个人数据的各项权利，防范、制止侵害个人数据权利的行为。个人数据处理应遵循合法、正当、必要和诚信原则，不得过度收集和非法获取个人数据，个人数据收集应限于实现处理目的的最小范围，存储不应超过法定期限。

核心原则 3： 维护数据公平和正义。

关键承诺：

坚持数据普惠性和包容性，防止数据偏见、边缘化和歧视，提升数字素养和能力以解决数据和知识鸿沟等问题。保障个人和机构平等获取具有公共利益属性数据、信息和知识并从中受益的权利。

核心原则 4： 确保有关主体责任和问责制。

关键承诺：

数据开发利用应符合法律法规和伦理规范。数据保护法需包含问责机制并确保得到落实。

核心原则 5： 坚持多方参与数据治理。

关键承诺：

发挥多方主体作用共促数据利用、发展和安全。加强制度能力和执法能力建设，提高公众数据保护能力，加强对数据保护的监督。

核心原则 6：增进数据领域国际合作与互信。

关键承诺：

加强数据安全治理和开发利用领域的国际合作，促进数据跨境依法有序自由流动。增进在保障数据安全和信息技术领域的互信。在联合国框架下推动数据领域国际规则制定，数据跨境流动规则应留有足够的政策空间。

四、关于网络人权

(Apply human rights online)

核心原则 1：确保互联网的关键基础设施和资源的连通性、韧性和安全。

关键承诺：

将互联网的关键基础设施和关键资源作为国际法或国际行为守则的公共核心。

核心原则 2：确立包容、平等参与制定互联网技术标准、监管机制和框架的环境。

关键承诺：

建立包容性和平等的环境、参与机制以及能力建设计划，例如开展技能和知识培训并提供资金，以鼓励和支持妇女、残疾人、老年人等各类弱势人群能够有效地平等参与互联网治理。

核心原则 3：强调人权的不可分割性，系统和全面的在数字领域增进经济、政治、社会、文化、环境权利。

关键承诺：

遵循联合国宪章为核心的国际法体系和国际法精神，关注人权法体系内的不可分割性与平衡，以及与其他法律部门之间的平衡，建立为确保所有人能享有互联网的可达、安全和益处构建良性的法律支撑体系。

核心原则 4：建立一个更具交互和包容性的参与性治理体系，改善全球和区域范围内治理体系的参与者和论坛的国际合作和战略参与。

关键承诺：

鼓励多利益相关方积极推进参与性治理体系的建设与完善，建立包容性和开放性的治理体系参与机制以及能力建设计划，建立治理参与者专家库，鼓励全球和区域范围内治理参与者的国际合作和战略参与。

核心原则 5： 数字包容。

关键承诺：

制定从发达到次发达国家/社群的技术转移计划。

五、关于引入对歧视和误导信息问责标准

(Introduce accountability criteria for discrimination and misleading content)

核心原则 1： 任何鼓吹战争的宣传，任何鼓吹民族、种族或宗教仇恨的主张，构成煽动歧视、敌视或暴力者，应以法律加以禁止。

关键承诺：

国家行为主体应该被禁止利用信息通信技术和信息通信网络干涉他国内政，破坏他国政治、经济和社会稳定。国家行为主体应该合作打击利用信息通信技术和信息通信网络从事犯罪和恐怖活动，或传播宣扬恐怖主义、分裂主义、极端主义以及煽动民族、种族和宗教敌意的行为。私营部门应该将关于反对战争宣传和民族、种族或宗教仇恨的原则纳入用户条款或社区规则，并在内容审核中进行贯彻。民间团体、技术社群以及学者应该共同努力，确保关于歧视和误导性内容的告知、标准以及救济机制公平合理运转。

核心原则 2： 坚持包容与责任原则。

关键承诺：

社交媒介平台应独立于政治、种族、民族、宗教和性别，包容多元化社群。社交媒介平台应建立解决个人和社会所面临风险的机制、标准和程序，来应对歧视和误导性内容。专业新闻和媒体在消除歧视和误导性信息方面发挥着重要作用，包括对既定新闻规范的承诺。

核心原则 3： 坚持加强数字素养教育原则。

关键承诺：

应加强数字素养技能教育，使公民能够对所遇到的内容或信息持更具批判性的意识，这有助于识别歧视和误导性内容，提高民主参与度。数字素养教育有助于提高在线安全意识，尤其是对弱势的个人和社群。针对不同人口群体的需求和风险所采取的各项举措需要保持敏感度。例如，针对青少年和老年人采取的不同方法，可对应不同的使用模式。数字素养教育课程应包含帮助儿童安全上网的数字素养技能，预防其受到虚假信息和误导性信息的伤害；并应为提升父母、其他监护人和教师的数字素养提供必要培训资源。

六、关于人工智能规制

(Promote regulation of artificial intelligence)

核心原则 1：包容性原则，涵盖促进福祉、公平公正、多样性、平衡性、可持续五个内涵。

核心原则 2：安全性原则，涵盖可靠性、可控性、可追溯性、可问责四个内涵。

核心原则 3：合作性原则，涵盖开放、可信、平等三个内涵。

核心原则 4：敏捷性原则，涵盖可对话、可借鉴、可互操作三个内涵。

关键承诺：

- **开展人工智能发展与治理国际性合作平台建设**

以“全球数字契约”建设进程为起点，在联合国框架下，类似于“联合国互联网治理论坛（IGF）”，成立专门讨论人工智能发展与治理的国际性会议平台，在理念共识、标准制定、规则协商、经验互鉴等方面推进国际合作。

- **开展人工智能发展与治理评估体系建设**

各国应积极探索并建立人工智能伦理影响评估框架与落实机制，在透明度协议、影响测试、外部审计、全生命周期流程监督等方面创新制度与工具设计。推动最佳实践的跨国分享与同行评议，开展国际对话并形成国际共识。

- **开展人工智能伦理教育与数字素养提升计划**

启动“人工智能教育普及计划”，减少因广泛采用人工智能而造成的数字不平等现象，并提升弱势群体、脆弱群体、

少数群体的人工智能应用能力。启动“人工智能伦理教育培训计划”，提升从业人员伦理水平，推动以负责任和合乎伦理方式发展与应用人工智能。