Commonwealth Cyber Governance Principles and Suggested Actions

PRINCIPLE	EXAMPLES OF PRACTICAL ACTIONS
We contribute to a safe and an effective global cyberspace: • as a partnership between public and private sectors, civil society and users, a collective creation; • with multi-stakeholder, transparent and collaborative governance promoting continuous development of cyberspace; • where investment in cyberspace is encouraged and rewarded; • by providing sufficient neutrality of the network as a provider of information services; • by offering stability in the provision of reliable and resilient information services; • by having standardisation to achieve global interoperability; • by enabling all to participate with equal opportunity of universal access; • as an open, distributed, interconnected Internet; • by providing an environment that is safe for its users, particularly the young and vulnerable; • made available to users at an affordable price.	• Promoting a culture of cybersecurity by raising awareness, setting standards and providing skills development. • Developing and tailoring national cybersecurity strategies that reflect the particular needs of each member nation while recognising its effect on global security. • Implementing working models for public-private collaboration in developing and operating cyberspace. • Identifying the cybersecurity aspects pertinent to the critical infrastructure and developing a collaborative solution with the private sector and other Commonwealth members to exceed minimum cybersecurity standards. • Developing understanding among policymakers of the key factors about network neutrality: the need for a standardised yet open cyberspace infrastructure, etc. • Collaborative working across governments and the private sector to provide reliable and affordable access initiatives. • Developing an understanding by government and private sector decision-makers about protecting market mechanisms for an effective cyberspace that is safe, secure, resilient and rewarding. • Preparing for, and introducing IPv6 as part of delivering sustainable broadband to citizens. • Participating in and supporting the work of the Internet.
Our actions in cyberspace support broader economic and social development by: • enabling innovation and sustainable development and creating greater coherence and synergy, through collaboration and the widespread dissemination of knowledge; • respecting cultural and linguistic diversity without the imposition of beliefs; • promoting cross-border delivery of services and free flow of labour in a multilateral trading system; • allowing free association and interaction between individuals across borders; • supporting and enhancing digital literacy; • providing everyone with information that promotes and protects their rights and is relevant to their interests, (e.g. supporting transparent and accountable government); • enabling and promoting multi-stakeholder partnerships; • facilitating pan-Commonwealth consultations and international linkages in a globally connected space that also serves local interests.	• Creating policy and regulatory frameworks that encourage innovation and entrepreneurship through the safe use of cyberspace for collaboration and the widespread dissemination of knowledge. • Creating safe, secure online markets for small, and medium-scale enterprises and rural enterprises. • Setting policy for the public sector, civil society and academia on publishing accessible and comprehensible online data. • Advice on creating open, transparent and accountable government using cyberspace. • Providing guidance and creating facilitating policy frameworks for the safe collection and use of electronic patient data to improve health outcomes. • Providing good practice for online publishing to encourage mutual understanding between cultures. • Agreeing common, practical cyberspace collaborative working tools to improve international working links.

COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION

The guide below offers examples of practical actions that can be implemented by nations to make the cyberspace safe, secure, resilient and rewarding, based on the Commonwealth principles. Against each of the four principles, this guide offers a corresponding set of practical actions, covering policy and technical measures including new technologies, legislation and regulations, organisational structures and international cooperation. For each of these actions, nations may seek capacity-building resources. Commonwealth members may also wish to prioritise their actions as short-term and long-term according to their circumstances, while recognising the impact of their actions on the global community.

PRINCIPLE	EXAMPLES OF PRACTICAL ACTIONS
We act individually and collectively to tackle cybercrime: • nations, organisations and society work together to foster respect for the law; • to develop relevant and proportionate laws to tackle cybercrime effectively; • to protect our critical national and shared infrastructures; • meeting internationally-recognised standards and good practice to deliver security; • with effective government structures working collaboratively within and between states; • with governments, relevant international organisations and the private sector working closely to prevent and respond to incidents.	• Implementing laws to fight cybercrime including computer and network misuse legislation, etc. • Establishing the necessary organisations, with appropriate authorities and resources to investigate and prosecute cybercrimes. • Strengthening mechanisms for international co-operation including exchange of information and provision of mutual assistance (adopting current Commonwealth frameworks such as the Harare Scheme on Mutual Assistance in Criminal Matters for the cyber age). • Identifying national critical information infrastructure and their regional linkages, developing strategies for their protection. • Developing sufficient expertise in computer forensics and the collection and safe custody of evidence to support criminal prosecution of cybercrimes. • Following best practice on setting up CERTs for national and local incident response. • Adopting measures to encourage sharing of incident information between CERTs. • Implementing international standards, like ISO-27000, in a proportionate and prioritised manner.
We each exercise our rights and meet our responsibilities in cyberspace • we defend in cyberspace the values of human rights, freedom of expression and privacy as stated in our Charter of the Commonwealth; • individuals, organisations and nations are empowered through their access to knowledge; • users benefit from the fruits of their labours; intellectual property is protected accordingly; • users can benefit from the commercial value of their own information; accordingly, responsibility and liability for information lies with those who create it; • responsible behaviour demands users all meet minimum cyber-hygiene requirements; • we protect the vulnerable in society in their use of cyberspace; • we, individually and collectively, understand the consequences of our actions and our responsibility to cooperate to make the shared environment safe; our obligation is in direct proportion to culpability and capability.	• Developing policy and providing guidance on achieving the balance between privacy and freedom of expression. • Developing policy and providing guidance on the balance between access to knowledge and protecting intellectual property online. • With ISPs, developing rules for minimum online hygiene requirements and responsible online behaviour, based on internationally-recognised good practice guides. • Tracking the emerging ideas on how individuals can monetise their data and providing advance assistance to citizens. • Contributing to international dialogues on respect for human rights and actively seeking to develop consensus. • Providing materials to teach children and adults about their rights and obligations in cyberspace. • Providing materials to teach children and adults how to operate safely in cyberspace. • Putting in place specific measures to protect children and other vulnerable users when online.