Commonwealth Cybergovernance Model

- Area: SET OF INTERNET GOVERNANCE PRINCIPLES
- Entitled by: Commonwealth Telecommunications Organisation
- Region: Commonwealth
- Organization: Commonwealth Telecommunications Organisation
- Sector: Technical community
- Keywords: Commonwelth, Cyber, governance, principles
- Doc Attached: Click here to see the doc 1
- Doc Attached: Click here to see the doc 2
- Doc Attached: Click here to see the doc 3

Abstract

Recognising the central importance of the internet to Commonwealth members and following the Abuja Declaration of Proposed Commonwealth Cybergovernance Model of 9 October 2013 and subsequent consultations, the Commonwealth Telecommunications Organisation offers this draft set of principles for consideration and adoption during the Commonwealth ICT Ministers Forum. The principles are intended to guide Commonwealth members to plan and implement practical actions in policy development, regulation and legislation, cross-border collaboration, capacity building, technical measures and other operational activities.

Document

Commonwealth ICT Ministers Forum 2014

Marlborough House, London

3 - 4 March 2014

Commonwealth Cybergovernance Model

1. Introduction

1.1. Recognising the central importance of the internet to Commonwealth members and following the *Abuja Declaration of Proposed Commonwealth Cybergovernance Model of 9 October 2013 and subsequent consultations*, the Commonwealth Telecommunications Organisation offers this draft set of principles for consideration and adoption during the Commonwealth ICT Ministers Forum. The principles are intended to guide Commonwealth members to plan and implement practical actions in policy development, regulation and legislation, cross-border collaboration, capacity building, technical measures and other operational activities.

2. Cyberspace – the internet and more

2.1. We are in an era of changing economic circumstances creating both opportunity and uncertainty, giving rise to new trade and economic patterns together with unforeseen threats to peace and security, and a surge in popular demands for democracy, human rights and for broadened social and economic opportunities. Previously unimagined access to information and communication between individuals across our planet is driving

economic and social development in the 21st century. Cyberspace [1] provides this access, helping us to bridge the digital divide while influencing every aspect of our economic and social activities. Cyberspace is becoming our global central nervous system. Cyberspace continues to develop at a pace unparalleled in our history - growth is anticipated from 2bn to 4bn users by 2020[2], many in developing countries. This pace of change necessitates urgent action in reaching consensus on Cybergovernance.

2.2. Its open, decentralised and distributed nature, that empowers the individual, has fostered innovation, collaboration and rapid development. Enjoyment of those benefits relies upon its safety, security and resilience. Cyberspace can also be a vehicle for crime, extremism and other social ills[3]. Governments, industry, civil society and users have a shared responsibility[4] to tackle those threats to society. Necessary security measures may be in tension with the very features that have made Cyberspace a success and, in determining an equitable balance, our behaviour in Cyberspace will benefit from our shared Commonwealth values that govern many aspects of our lives.

3. Applying Commonwealth values in Cyberspace

3.1. The Commonwealth Charter of March 2013 reflects the values and aspirations which unite the Commonwealth - democracy, development, human rights and the rule of law. The Charter expresses the commitment of member states to the development of free and democratic societies and the promotion of peace and prosperity to improve the lives of all peoples of the Commonwealth. It also acknowledges the role of civil society in supporting the goals and values of the Commonwealth.

3.2. The principles concerning our use of Cyberspace today and the evolving nature of Cyberspace tomorrow should be derived from, should respect and reflect our shared Commonwealth values as set out in the Commonwealth Charter. Within the context of the Charter as a whole, we identify the key characteristics, which led to our principles, as exemplified in Appendix 1. This analysis is based on the principle that what is unacceptable off-line is unacceptable on-line. Priorities for practical action, in accordance with these principles, will depend on the prevailing circumstances in each country.

4. Commonwealth principles for the use of Cyberspace

4.1. As we operate in Cyberspace and work with others to shape its continuing development, we will use the following principles to guide our decisions, actions and demonstrate our progress towards meeting these principles. The principles are best considered collectively and not each in isolation without regard to the whole because frequently some are in tension with each other. We reiterate the urgency with which these issues need to be addressed.

Principle 1: 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 the 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.

Principle 2: Our actions in Cyberspace support broader economic and social development

- by enabling innovation and sustainable development, 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 multi-lateral 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, for example to support 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.

Principle 3: We act individually and collectively to tackle cybercrime[5]

- 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.

Principle 4: 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.

5 Practical application of these principles

5.1. Each Commonwealth member may find it beneficial to develop individually, a whole of government strategy, reflecting the many facets in making Cyberspace safe, secure, resilient and rewarding, that will address unique local needs of countries with their different regions, sectors and industries and deliver their particular economic and social priorities.

5.2. Appendix 2 offers a guide to sample practical actions that can be taken by Commonwealth members, based on these principles. Appendix 3 provides a list of organisations offering practical guidance on Cybersecurity. Appendix 2 and 3, for guidance only, are illustrative and new initiatives in this fast-moving topic may not be reflected.