The Commonwealth

COMMONWEALTH
HEADS OF GOVERNMENT MEETING
LONDON 2018

# Commonwealth Cyber Declaration

***Recognising*** that the development of cyberspace has made a powerful contribution to the economic, social, cultural and political life of the Commonwealth;

***Underlining*** that cyberspace provides a common space, within which the diversity and richness of Commonwealth identities can be expressed;

***Emphasising*** the critical role of cyberspace in connecting all Commonwealth member countries, in particular small island developing states, to global value chains in the context of an increasingly globalised economy;

***Recalling*** the Commonwealth Charter commitment to strengthening the use of information and communication technologies, while enhancing their security, for the purpose of the sustainable development of our societies;

***Recognising*** the threats to stability in cyberspace and integrity of the critical infrastructure and affirming our shared commitment to fully abide by the principles and purposes of the Charter of the United Nations to mitigate these risks;

***Building*** on the principles expressed in the 2014 Commonwealth Cyber governance Model adopted by the Commonwealth ICT Ministers Forum and our shared commitment to Commonwealth values of human rights, tolerance, respect and understanding, freedom of expression, rule of law, good governance, sustainable development and gender equality;

***Underscoring*** our shared interest in protecting the security of our networks, security of data, the people that use them, and the services that run on them;

We, as Commonwealth Heads of Government, commit to:

## A cyberspace that supports economic and social development and rights online

Recognising the potential for a free, open, inclusive and secure cyberspace to promote economic growth for all communities and to act as an enabler for realisation of the Sustainable Development Goals across the Commonwealth, we:

*1.* *Recognise and support* cyberspace as an enabling environment to promote investment and intra-Commonwealth trade in goods and services through open markets, the free flow of information, innovation, and fair competition.

*2.* *Commit to* promote interoperable and global technical standards, through appropriate consultative processes involving industry, academia, governments and other relevant stakeholders, recognising that standards should be open, foster security and trust and not act as barriers to trade, competition or innovation.

3. *Highlight* the importance of common standards and the strengthening of data protection and security frameworks, in order to promote public trust in the internet, confidence for trade and commerce, and the free flow of data.

4. *Acknowledge* the importance of tolerance, respect for diversity, and understanding in cyberspace.

*5.* *Affirm* that the same rights that citizens have offline must also be protected online.

*6.* *Commit* to limit the circumstances in which communication networks may be intentionally disrupted, consistent with applicable international and domestic law.

*7.* *Recognise* that without cybersecurity citizens are at risk of crime or exploitation, and *commit* to strengthening legislative, social and educational measures that protect the vulnerable.

*8.* *Recognise* that access to information and digital literacy can be a powerful catalyst for economic empowerment and inclusion, and *commit* to take steps towards expanding digital access and digital inclusion for all communities without discrimination and regardless of gender, race, ethnicity, age, geographic location or language.

9. *Emphasise* that enhanced digital inclusion of young people in the Commonwealth can contribute in a positive way to their education, social engagement and entrepreneurship.

**Build the foundations of an effective national cyber security response**

Recognising the need for individual and collective action to tackle cybercrime and protect critical national infrastructure, we:

1. *Note* the importance and involvement of all stakeholders within their respective roles and responsibilities in the good governance of cyberspace.

2. *Highlight* the importance of national cybersecurity strategic planning and establishing incident response capabilities, supported by appropriate legislation and a law enforcement and criminal justice system capable of addressing cybercrime.

*3.* *Commit* to support businesses to implement appropriate measure to protect themselves and their customers from cybersecurity threats.

4. *Commit* to work towards the development and convergence of approaches for internet-connected devices and associated services, in order to promote user security by default.

5. *Encourage* investment in cybersecurity and cyber hygiene skills, and to develop skills in the workforce, particularly for women and girls, and public awareness to help the public adopt secure online behaviours and protect themselves from cybercrime.

6. *Recognise* the potential for sharing of information across the Commonwealth for improving cooperation between government, law enforcement and industry, with due regard for necessary and proportionate safeguards.

7. *Commit* to exploring options to deepen cooperation on cybersecurity incidents and responses between Commonwealth member countries, including through the sharing of information about threats, breaches, vulnerabilities, and mitigation measures.

8. *Note with concern* the challenges faced by Commonwealth developing member countries, particularly less developed countries and small island developing states. *Commit* to invest in cybersecurity capacity building, including through the transfer of knowledge and technology on mutually agreed terms, the development of skills and training, the promotion of education and research, awareness raising, and access to good practice.

**Promote stability in cyberspace through international cooperation**

Recognising the importance of international cooperation in tackling cybercrime and promoting stability in cyberspace, we:

1. *Commit* to the establishment of effective and proportionate domestic cybercrime and cybersecurity frameworks that take into account principles in existing international instruments, acknowledging the evolving tactics of cybercriminals and the transnational nature of cybercrime. *Commit* to use national contact points and other practical measures to enable cross-border access to digital evidence through mutually agreed channels to improve international cooperation to tackle cybercrime.

2. *Commit* to work towards common standards, harmonised legal approaches and improved interoperability, including through the use of Commonwealth model laws; and *commit* to considering the potential for further Commonwealth cooperation in this regard, including the possible coordination of common positions in international fora.

3. *Commit* to promote frameworks for cyberspace, including the applicability of international law, agreed voluntary norms of responsible state behaviour, and the development and implementation of confidence building measures to encourage trust, cooperation and transparency, consistent with the 2015 Report of the United Nations Group of Governmental Experts on Developments in the

Field of Information and Telecommunications in the Context of International security (UNGGE).

4. *Commit* to move forward discussions on how existing international law, including the Charter of the United Nations, and applicable international humanitarian law, applies in cyberspace in all its aspects.

United Kingdom
20 April 2018

## Implementation Plan 2018 - 2020

In order to ensure implementation of the Commonwealth Cyber Declaration, and welcoming the existing support provided to Commonwealth member countries by the Commonwealth Secretariat through the Commonwealth Cybercrime Initiative, working in partnership with the Commonwealth Telecommunications Organisation, Heads of Government endorse the following implementation plan:

1. Member countries will provide support, as appropriate, to encourage all Commonwealth member countries to undertake voluntarily a national cybersecurity capacity review by the Commonwealth Heads of Government meeting in 2020, in order to understand the current level of cybersecurity capabilities and identify priority needs for capacity building.

2. Working with relevant international organisations, the private sector, academic institutions, Commonwealth initiatives and their stakeholders, Commonwealth member countries will:

- Work to increase cooperation within the Commonwealth to help all members put in place the foundations of an effective national cybersecurity response, including planning, incident response and cybercrime legislation; and

- Help build capacity through knowledge transfer, awareness raising, access to good practice and by investing in targeted capacity building efforts, including in law enforcement and criminal justice.

3. Member countries will work together to identify priority areas and themes for capacity building efforts. These may include in areas such as:

- Strengthening cybersecurity strategies, policies and legislation through the development and sharing of models and good practice;

- Providing training and skill development for more effective law enforcement and criminal justice responses to cybercrime;

- Improving cyber incident response capabilities;

- Enhancing the protection of election systems through better cybersecurity;

- Improving cybersecurity skills and knowledge through public awareness campaigns and investing in improved digital skills in the workforce;

- Strengthening cybersecurity within the banking and finance system, including the security of FinTech and digital currencies;

- The organisation of national, regional and pan-Commonwealth cybersecurity events in order to share knowledge and good practice; and

- Identifying and accessing sustainable funding sources for cybersecurity work in the Commonwealth.