



# Draft Internet Code of Practice 2025

October 2025

# Content

## Chapter 1: Introduction

1.1 Preamble .....	5
1.2 Legal Basis for the Code .....	5
1.3 Objectives of the Code .....	6
1.4 Application and Scope of the Code .....	6
1.5 Right of Consumers to Open Internet Access .....	7
1.6 International Cooperation and National Collaboration .....	7

## Chapter 2: Standards for Open Internet Access

2.1 Transparency .....	8
2.2 No Discrimination .....	8
2.3 No Blocking .....	8
2.4 No Throttling .....	8
2.5 No Preferential Data Prioritization .....	8
2.6 Zero-Rating .....	9
2.7 Traffic Management Practices .....	9

## Chapter 3: Cybersecurity, Privacy and Data Protection

3.1 Cybersecurity .....	10
3.2 Compliance with Statutes and Regulations .....	10
3.3 Data Security .....	10
3.4 Data Breach Notifications .....	10
3.5 Transactional Data Management .....	10

## Chapter 4: Child Online Safety – Online Protection of Minors and Ors

4.1 Incorporation of Child Online Protection policies into T&Cs of Service.....	11
4.2 Reporting Mechanism for Child Sex Abuse Content .....	11
4.3 Blocking of Access to Child Sexual Abuse Content Mechanism .....	11
4.4 Parental Control Measures .....	11-12

4.5 Education of Parents, Guardian and Minors .....	12
---	----

## **Chapter 5: Network Governance Rules**

5.0 Safeguards against Unsolicited Internet Communications .....	13
5.1 Incorporation of Anti-Spam Policies into Terms and Conditions of Service .....	13
5.2 Spam Filters .....	13
5.3 Obligations pertaining to Unlawful content .....	13
5.3.1 No Monitoring Obligations .....	13
5.3.2 Procedure for Reporting Unlawful Content .....	14
5.3.3 Take down Notice .....	14
5.3.4 Collaborations with Law Enforcement on Unlawful Content .....	14
5.3.5 Obligations of Internet Access Service Provider under Existing Laws .....	14
5.4 Deployment of Artificial Intelligence and Emerging Technologies .....	15
5.4.1 Deployment of Artificial Intelligence on the Network .....	15
5.4.2 Regulatory Requirements for the Deployment of Artificial Intelligence .....	16
5.4.3 Governance Standards.....	16

## **Chapter 6: Online Digital Platforms Governance Rules**

6.1 Online and Digital Communications Platforms .....	17
6.1.1 Community Rules and Guidelines .....	17
6.1.2 Rendition Governance Rules .....	17
6.1.3 Governance Interface and Channel .....	17
6.2 Digital Service Provision .....	17
6.2.1 Community Rules and Guidelines .....	17
6.2.2 Rendition Governance Rules .....	18
6.2.3 Governance Interface and Channel .....	18
6.3 Application Service Provision .....	18
6.3.1 Community Rules and Guidelines .....	18
6.3.2 Rendition Governance Rules .....	18
6.3.3 Governance Interface and Channel .....	18

6.3.4 Governance Standards .....	18
----------------------------------	----

## Chapter 7: Compliance Monitoring and Enforcement

7.1 Monitoring and Enforcement .....	19
7.2 Consumer Web Portal.....	20
7.3 Rendition Requirements .....	20

## Chapter 8 Interpretations and Code review

8.1 Interpretation of Key terms/ words.....	21
8.2 Code Review .....	24
8.3 Transitional Provisions.....	24

## Schedules

**First Schedule:** Internet Access Service Provider Rendition Template

**Second Schedule:** Online Platform Rendition Template

**Third Schedule:** Code Compliance Rendition Template

# Chapter One

## 1.1 Preamble

The Internet can provide enormous benefits to the Nigerian public as a source of information, education, research, commerce, communication, and entertainment, and as a key driver for innovation and technological advancement. However, the Internet also includes content that some users might find objectionable and would not want themselves, their children, or even society at large, exposed to.

While an Open Internet is key for successfully driving innovation, there are several factors to be considered in its promotion, such as privacy and data protection, child online protection, objectionable content, unsolicited communications, and traffic management practices that are considered necessary in order to maintain network efficiency. Furthermore there are factors related to deployment of emerging technologies by licensees of the Commission that may impact on both access and quality of experience on the Internet. Hence the need to set out governance principles and acceptable approaches to ensure hygienic and well managed use of the internet by all subscribers and consumers of the Nigerian Communications Sector.

To this end, the Nigerian Communications Commission, in accordance with its authority to regulate the communications sector in Nigeria as expressed in the Nigerian Communications Act 2003, had published an Internet Code of Practice in 2019. The Commission initiated a Consultation Process in July 2025 that led to engagement of National and International stakeholders on five regulatory proposals to improve the Code. Consequently, the Commission hereby publishes this amended Internet Code of Practice to define the rights and obligations of Internet Access Service Providers with regard to the issues therein. It is also intended to guide the activities of the licensees of the Commission on their management of subscribers and consumers of communications services in Nigeria.

## 1.2 Legal Basis for the Code

This Code is issued as a Guidelines in line with the provisions of Section 70 of the Nigerian Communications Act 2003 (Act) that empowers the Commission to issue subsidiary legislations on all matters pertaining to the provisions of the Act and its effective implementation. Furthermore in Section 4 (2) the Act requires the Commission to exercise its powers efficiently, effectively and in a non-discriminatory and transparent manner and in a way that is best calculated to ensure that there are provided throughout

Nigeria, subject to the regulatory controls specified in the Act, all forms of communications services, facilities and equipment on such terms and subject to such conditions as the Commission may from time to time specify.

Lastly the Act in Section 146 (1) states that a licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content application service that he provides from being used in, or in relation to, the commission of any offence under any law in operation in Nigeria.

### 1.3 Objectives of the Code

The specific objectives of the Code are to:

- a) Protect the right of Internet users to an Open Internet;
- b) Provide clear guidelines to Internet Access Service Providers on the use of traffic management practices;
- c) Outline the obligations of Internet Access Service Providers in relation to the protection of consumers' personal data;
- d) Outline the obligations of Internet Access Service Providers in the handling of offensive and potentially harmful content, and the protection of minors and vulnerable audiences online;
- e) Ensure adequate safeguards are put in place by Internet Access Service Providers against unsolicited Internet communications.
- f) Ensure that Online Platforms and Digital Services align their activities to the regulatory environment through cohabitating governance rules that lay out guiding principles in that regard.

### 1.4 Application and Scope of the Code

This Code of Practice is applicable to:

- a) Internet Access Service Providers (as defined within the Code);
- b) The provision of Internet Access Services within Nigeria.
- c) All impacted entities that provide or offer services that fall within the regulatory purview of the Nigerian Communications Act 2003

## **1.5 Right of Consumers to Open Internet Access**

The Code upholds the consumer's right to an Open Internet. Hence:

- a) Internet users have the right to access and distribute information and content, use and provide applications and services, and use appropriate terminal equipment of their choice.
- b) No lawful content, applications or services shall be blocked or made unavailable to users of Internet services.
- c) No lawful content, applications or services shall be discriminated against by an Internet Access Service Provider.
- d) Where traffic management practices are required in order for the efficient operation of the network, an Internet Access Service Provider shall be completely transparent about what practices are in place and how the consumers' services are affected.

## **1.6 International Cooperation and National Collaboration**

- I. The Commission shall engage International Agencies, Regulators and Cross-National bodies in deepening the governance of Online and Digital Services through Peer Reviews and coordinated governance engagements.
- II. The Commission shall collaborate with Relevant Organisations as defined in Chapter Eight of this Code in applying the governance rules enshrined in Chapter Six of this Code and provide monitoring and enforcement support to other agencies of the government.

## Chapter Two

### Standards for Open Internet Access

#### 2.1 Transparency

- a) An Internet Access Service Provider shall disclose on its website and in all service agreements, full and accurate information regarding the performance, technical and commercial terms of its Internet Access Services in a manner sufficient for consumers and third-party content providers to make informed choices regarding their use of such services.
- b) Any traffic management practices employed by an Internet Access Service Provider for the purposes of network optimization shall be fully publicly disclosed, including:
- I. The specific reason(s) why the traffic management practices are required;
  - II. The specific goal(s) of the practices implemented;
  - III. The manner in, and the extent to which those practices may affect the Internet Access Services.

#### 2.2 No discrimination

An Internet Access Service Provider shall treat all lawful traffic within the same service category equally, without discrimination, restriction or interference, irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.

#### 2.3 No blocking

An Internet Access Service Provider shall not block any lawful content, applications, services, or non-harmful devices, with the exception of reasonable network management.

#### 2.4 No throttling

An Internet Access Service Provider shall not impair or degrade lawful internet traffic on the basis of internet content, source, destination, application, or service, or use of a non-harmful device, with the exception of reasonable network management.

#### 2.5 No preferential data prioritization

An Internet Access Service Provider shall not engage in preferential data prioritization under any circumstances.



## 2.6 Zero-Rating

Zero-rating may be permissible to the extent that it furthers the objectives of the Act, particularly Section 1 (c), and policy objectives of Universal Access contained in the National Information and Communications Technology Policy 2012 and the Nigeria ICT Roadmap 2017 - 2020, in accordance with the provisions of the Competition Practice Regulations 2007 as may be amended by the Commission from time to time, and with the approval of the Commission.

## 2.7 Acceptable Traffic Management Practices

a) Circumstances that may warrant the use of reasonable network management by an Internet Access Service Provider are as follows:

- I. In order to preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of internet users;
- II. In order to prevent impending network congestion or mitigate the effects of temporary network congestion, provided that equivalent categories of traffic are treated equally;
- III. In order to comply with a law, court order or regulatory obligation.

b) Reasonable network management practices in this context shall demonstrate the following characteristics:

- I. There shall be a legitimate and demonstrable technical need for the practice;
- II. The practice shall have a specific and stated technical goal;
- III. The effect of the practice shall be proportional to the need it intends to address, and considered a reasonable effect by the majority of consumers;
- IV. There shall be full disclosure with regard to the practice, in a manner sufficient for consumers to develop an informed opinion on whether, when, and how the practice will affect their service.
- V. The practice shall be based on globally accepted standards.

## 2.8 Electronic Addressing Management

I. All IASPs are to document and submit all Internet Protocol (IP) addresses deployed on their networks and such submission should be made to the Commission on Quarterly basis.

II. All IASPs are to maintain utilization records of all IP addresses on their network and shall submit same to the Commission on Quarterly basis.

III. All IASPs shall report to the Commission any IP address deployed in a manner that breaches this Code and the provisions of Section 128 of the Nigerian Communications Act 2003.

## Chapter Three

### Cyber Security, Privacy and Data Protection Obligations

#### 3.1 Cyber Security

All Internet Access Service Providers are to implement the Cyber Security Framework that is issued by the Commission to all its licensees. This Framework shall provide the strategic and operational baselines for the Nigerian Communications Sector.

#### 3.2 Compliance with Statutes and Regulations

An Internet Access Service Provider shall comply with the provisions of the Nigerian Data Protections Act 2023 and Part VI of Schedule 1 of the Consumer Code of Practice Regulations 2024 or as may be amended by the Nigerian Communications Commission, on Protection of Consumer Information.

#### 3.3 Data Security

- a) An Internet Access Service Provider shall take reasonable measures to protect customer information from unauthorized use, disclosure, or access.
- b) The security measures taken by an Internet Access Service Provider to implement the requirement set forth in this section shall appropriately take into account each of the following factors;
  - I. The sensitivity of the data collected; and
  - II. Technical feasibility.

#### 3.4 Data Breach Notifications

- a) *Customer Notification:* An Internet Access Service Provider shall notify affected customers of any breach relating to the customer's information within 48 hours of its occurrence, by email and text message.
- b) *Notification of the Commission:* An Internet Access Service Provider shall formally notify the Commission in writing of any breach no later than 48 hours after the Internet Access Service Provider reasonably determines that a breach has occurred.

#### 3.5 Transactional Data Management

An Internet Access Service Provider shall not allow the harvesting of transactional data on its network or access by a third party without the prior written approval of the

Commission. The Commission's approval shall be preceded by an impact assessment and review of such access and its potential effects on national considerations, consumer information and personal data.

## Chapter Four

### Child Online Safety - Online Protection of Minors and other Vulnerable Dependants

#### 4.1 Incorporation of Child Online Protection Policies into Terms and Conditions of Service

- a) An Internet Access Service Provider shall include in its Terms and Conditions of Service, a clear set of rules for the use of the Service that comply with the Cybercrime Act (Amended) 2024, Child Online Protection Policy and all other applicable laws and regulations.
- b) The Terms and Conditions shall be published prominently on the Internet Access Service Provider's website and on all service agreements, either electronic or otherwise.
- c) All Internet Access Service Providers and Impacted Entities as defined in Chapter Eight of this Code shall offer consistent and simple-to-enable parental control tools.
- d) All Internet Access Service Providers and Impacted Entities as defined in Chapter Eight of this Code shall offer multilingual, simple guidance on usage and safety
- e) All Internet Access Service Providers and Impacted Entities as defined in Chapter Eight of this Code shall ensure that as part of parent control measures have a default setting of “opt-in” before commencement of services to minors and vulnerable dependants.

#### 4.2 Reporting Mechanism for Child Sex Abuse Content

An Internet Access Service Provider shall provide clear and adequate directions to its customers for reporting child sexual abuse content to the Commission.

#### 4.3 Blocking of Access to Child Sexual Abuse Content

An Internet Access Service Provider shall have measures in place for the immediate blocking of access to child sexual abuse content, once notified by the Commission.

#### 4.4 Parental Control Measures

- a) Optional Parental Control Measures (PCMs), such as content filters, usage monitoring tools, and usage control tools, shall be offered either directly to customers or via the provision of information in a reasonably prominent position on the Internet Access Service Provider's website regarding third party websites that provide

a means for consumers to have access to or acquire parental control tools.

b) Where an Internet Access Service Provider provides PCMs directly to customers, the Internet Access Service Provider shall take reasonable steps to ensure that the customer is advised, at the point of sale, methods by which the PCMs can be regularly updated, and further, where information can be obtained regarding the continuing availability of the PCMs. Reasonable steps may include the provision of the information or a link to the information on/from the webpage from which the PCMs are offered to customers.

c) When offering PCMs to customers pursuant to Paragraph 4.3 (a), Internet Access Service Providers shall not offer the PCMs in a way that would involve a contravention of any provision of the Competition Practice Regulations 2007 as may be amended by the Commission from time to time.

d) Internet Access Service Providers shall take reasonable steps to ensure that customers who elect to use PCMs fully understand how to use them to manage their children's (and vulnerable dependants') access to Internet content and Internet resources.

#### 4.5 Education of Parents, Guardians, and Minors

a) *Parents and Guardians*: Internet Access Service Providers shall take reasonable steps to ensure that adult customers are provided with information that will help them understand the risks that minors and other vulnerable dependants may be susceptible to online and how to mitigate such risks. The information provided may include but not limited to:

I. The general types of content available online that may not be age-appropriate for minors;

II. Other risks that minors and vulnerable dependants may be exposed to online, such as sexual predators and grooming, radicalization and recruitment for terrorist activities, and what signs to watch out for;

III. The types of risky online behaviour that should be discouraged in minors and vulnerable dependants;

IV. How to report inappropriate or unlawful content and misuse of the Service;

V. The Parental Control Measures available and how to use them.

b) *Minors and Vulnerable Dependants*: Internet Access Service Providers shall take reasonable steps to provide parents and guardians of minors and other vulnerable dependants using their services with information with which to educate their ward(s) on online safety. The information provided may include instructions such as:

- I. Warnings never to give out personal information, such as their physical location and other details, to strangers online;
- II. Warnings never to meet in person with online acquaintances without parental consent and/or the presence of a parent or guardian;
- III. Advice on risky online behaviours to avoid, such as obliging requests from online acquaintances for questionable actions, pictures or videos of themselves;
- IV. Instructions to inform a parent, guardian, or trusted adult of any online interaction that makes them feel uncomfortable in any way.

## Chapter Five

### Network Governance Rules

#### 5.0 Safeguards against Unsolicited Internet Communications

##### 5.1 Incorporation of Anti-Spam Policies into Terms and Conditions of Service

- a) An Internet Access Service Provider shall include in its Terms and Conditions of Service, rules prohibiting the use of the Service to spam other users of the Internet.
- b) The Terms and Conditions shall be published prominently on the Internet Access Service Provider's website and on all service agreements, either electronic or otherwise.

##### 5.2 Spam Filters

- a) Optional spam filters may be offered either directly to customers or via the provision of information in a reasonably prominent position on the Internet Access Service Provider's website regarding third party websites that provide a means for consumers to have access to or acquire spam filters.
- b) Where an Internet Access Service Provider provides client-side spam filters directly to customers, it shall ensure that the customer is advised at the point of sale, methods by which the spam filter can be regularly updated, and further, where information can be obtained regarding the continuing availability of the spam filter.
- c) When offering spam filters to customers pursuant to Paragraph 5.2 (a), Internet Access Service Providers shall not offer the filter in a way that would involve a contravention of any provision of the Competition Practice Regulations 2007 as may be amended by the Commission from time to time.

#### 5.3 Obligations pertaining to unlawful Content

##### 5.3.1 No Monitoring Obligation

An Internet Access Service Provider is generally under no obligation to monitor content which it stores or transmits when providing Internet Access Services, nor are they under any obligation to seek facts or circumstances indicating unlawful activity, except when acting under instruction from the Commission or relevant law enforcement agency.

### **5.3.2 Procedure for Reporting Unlawful Content**

An Internet Access Service Provider shall provide clear and adequate directions to its customers for reporting unlawful content to the Commission.

### **5.3.3 Takedown Notice**

- a) Upon determination by the Commission that the content reported under Paragraph 5.3.2 above is indeed unlawful, the Commission shall issue a takedown notice to all Internet Access Service Providers to deny or disable access to the content. The Internet Access Service Providers shall be expected to comply with such takedown notice within 24 hours of receipt of the notice.
- b) The Commission may issue takedown notices to an Internet Access Service Provider on a particular content or specific content that relates to it alone in cases where such content is reported under Paragraph 5.3.2 above as unlawful and the Internet Access Service Provider shall be expected to comply with such takedown notice within 24 hours of receipt of the notice.
- c) All takedown procedures on all the networks provided by the Internet Access Service Providers shall be in line with the provisions of this Code and all statutory and regulatory requests by relevant agencies shall be in line with the procedures herein set out.
- d) A person who is aggrieved or whose interest is adversely affected by any takedown notice issued by the Commission pursuant to this Paragraph may appeal the decision in accordance with the provision of Chapter V, Part X of the Act.
- e) Relevant Organisations as defined in Chapter Eight of this Code can initiate Takedown procedures through the Commission and the provisions of this Code shall apply to such requests.

### **5.3.4 Collaboration with Law Enforcement on Unlawful Content**

In the event of a criminal investigation into unlawful content, Internet Access Service Providers shall reasonably support the relevant law enforcement agencies by gathering and providing applicable evidence as required.

### **5.3.5 Obligations of Internet Access Service Providers under existing laws**

Internet Access Service Providers shall also comply with the provisions within the Act, the Cybercrime Act (Amended) 2024, terms and conditions of their licence and all applicable Regulations and Guidelines.



## 5.4 Deployment of Artificial Intelligence and Emerging Technologies

Internet Access Service Providers shall ensure that all deployment of artificial intelligence tools and applications as well as emerging technologies are in line with the governance rules set in this Code.

### 5.4.1 Deployment of Artificial Intelligence on the Network

An Internet Access Service Provider shall notify the Commission prior to deploying Artificial Intelligence tools, applications and solutions that relate to all its network management and customer engagement processes. This notification shall include the following details:

- I. The services to be covered or affected by such tools, applications or solutions.
- II. Existing services that may be replaced or supplanted by the new tools, applications or solutions.
- III. Potential upgrades or changes to the tools, applications or solution.
- IV. Implementation timelines, lifespans and sunseting principles applicable to such tools, applications or solutions.

Provided that same notification will be required for the deployment of any emerging technological tool, application or solution.

### 5.4.2 Regulatory Requirements for the Deployment of Artificial Intelligence

The following regulatory requirements apply to all Internet Access Service Providers deploying artificial intelligence or any emerging technology on their networks

- I. The Internet Access Service Provider shall notify subscribers and consumers that will be impacted by the deployment of such artificially intelligent tools, applications and solutions, particularly for non-human interfaces on consumer complaint or redress platforms.
- II. The Internet Access Service Provider shall ensure that the deployment of such artificially intelligent tools, applications and solutions will not impact on its own network integrity or its connectivity with other Internet Access Service Providers.
- III. The Internet Access Service Provider shall ensure that such artificially intelligent tools, applications and solutions are not breaching operational requirements set in the Cyber Security Framework issued by the Commission or accessing consumer data without consent or regulatory approvals.
- IV. The Internet Access Service Provider shall maintain a capability to withdraw such artificially intelligent tools, applications and solutions where there is a regulatory

determination that requires immediate removal or cessation of its functions.

V. The Commission may issue compliance guidance, directives or further requirements on artificially intelligent tools, applications and solutions from time to time to complement the provisions of this Code.

#### 5.4.3 Governance Standards

The Commission may issue governance standards and requirements from time to time to achieve the implementation of the provisions of this Chapter and these standards will be developed in consultation with all licensees and impacted entities.

## Chapter Six

### Online and Digital Platforms Governance Rules

#### 6.1 Online and Digital Communications Platforms

These provisions apply to entities as defined in Chapter Seven of this Code and the governance rules will provide baseline engagement parameters for managing their activities that are within the purview of the Nigerian Communications Act 2003.

##### 6.1.1 Community Rules and Guidelines

I. All Online and Digital Communications Platforms shall have Community Rules or Guidelines that align with the provisions of Section 146 the Nigerian Communications Act 2003 as it relates to protection of National Interest.

II. All Online and Digital Communications Platforms shall submit their Community Rules or Guidelines to the Commission within six months of the issuance of this revised Code.

##### 6.1.2 Rendition Governance Rules

All Online and Digital Communications Platforms shall make minimal rendition to the Commission on bi-annual basis in the format set out in the Second Schedule to this Code.

##### 6.1.3 Governance Interface and Channel

All Online and Digital Communications Platforms shall set up and provide a channel of engagement with the Designated Online Governance Officer (DOGO) appointed by the Commission in its relevant Department. This Channel shall be the primary engagement point for managing harmful content, disinformation, fraudulent activities and unlawful content.

#### 6.2 Digital Service Provision

These provisions apply to entities as defined in Chapter Seven of this Code and the governance rules will provide baseline engagement parameters for managing their activities that are within the purview of the Nigerian Communications Act 2003.

##### 6.2.1 Community Rules and Guidelines

I. All Digital Service Providers shall have Community Rules or Guidelines that align with the provisions of Section 146 the Nigerian Communications Act 2003 as it relates to protection of National Interest.

II. All Digital Service Providers shall submit their Community Rules or Guidelines to the Commission within six months of the issuance of this revised Code.

## **6.2.2 Rendition Governance Rules**

All Digital Service Providers shall make minimal rendition to the Commission on bi-annual basis in the format set out in the Second Schedule to this Code.

## **6.2.3 Governance Interface and Channel**

All Online and Digital Communications Platforms shall set up and provide a channel of engagement with the Designated Online Governance Officer (DOGO) appointed by the Commission in its relevant Department. This Channel shall be the primary engagement point for managing harmful content, disinformation, fraudulent activities and unlawful content.

## **6.3 Application Service Provision**

These provisions apply to entities as defined in Chapter Seven of this Code and the governance rules will provide baseline engagement parameters for managing their activities that are within the purview of the Nigerian Communications Act 2003.

### **6.3.1 Community Rules and Guidelines**

I. All Application Service Providers shall have Community Rules or Guidelines that align with the provisions of Section 146 the Nigerian Communications Act 2003 as it relates to protection of National Interest.

II. All Applications Service Providers shall submit their Community Rules or Guidelines to the Commission within six months of the issuance of this revised Code.

### **6.3.2 Rendition Governance Rules**

All Application Service Providers shall make minimal rendition to the Commission on bi-annual basis in the format set out in the Second Schedule to this Code.

### **6.3.3 Governance Interface and Channel**

All Online and Digital Communications Platforms shall set up and provide a channel of engagement with the Designated Online Governance Officer (DOGO) appointed by the Commission in its relevant Department. This Channel shall be the primary engagement point for managing harmful content, disinformation, fraudulent activities and unlawful content.

### **6.3.4 Governance Standards**

The Commission may issue governance standards and requirements from time to time to achieve the implementation of the provisions of this Chapter and these standards will be developed in consultation with all licensees and impacted entities.

## Chapter Seven

### Compliance Monitoring and Enforcement

#### 7.1 Monitoring and Enforcement

##### 7.1.1 The Commission

a) The Commission shall monitor and ensure compliance with the Code:

I. At the request of the Commission, entities subject to the application of the Code shall make available to the Commission information relevant to their obligations under the Code. In particular, Internet Access Service Providers may be required by the Commission to provide information concerning the management of their network capacity and traffic, as well as justifications for any traffic management measures applied. Those Internet Access Service Providers shall provide the requested information in accordance with the time-limits and the level of detail required by the Commission.

II. Whenever the Commission determines that an entity subject to the provisions of the Code is in breach or fails to observe the principles of the Code, the Commission shall notify the entity concerned specifying the areas of non-compliance or non-observance and the specific action(s) needed to remedy the non-compliance or non-observance. The entity shall perform the action(s) specified and indicate its subsequent compliance with the Code in a report submitted to the Commission within fourteen days.

b) The monitoring and enforcement of the Code shall be exercised in accordance with the Nigerian Communications (Enforcement Processes, etc.) Regulations 2019. With respect to any penalties for contravention of applicable provisions, the Commission shall be guided by the considerations set out in the Regulations.

##### 7.2 Consumer Web Portal

I. The NCC Consumer Web Portal shall be updated to accept complaints from consumers about non-compliance with the Code from their Internet Access Service Provider.

II. Complaints submitted to the portal shall be reasonably investigated

by the Commission in accordance with its complaints adjudicatory processes.

III. Request for any actions or approvals with regard to the Code shall be channeled to the appointed DOGO through the Office of Executive Vice Chairman of the Nigerian Communications Commission.

### 7.3 Rendition Requirements

I. All Internet Access Service Providers shall render reports to the Commission on compliance with the Code on biannual basis and the rendition shall be through the template provided in the First Schedule to this Code.

II. All Internet Access Service Providers and impacted entities shall submit compliance reports with all request made by the Commission on any matter provided in this Code and the compliance status shall be rendered through the Template provided in the Third Schedule to this Code.

III. All impacted entities shall render reports to the Commission on adherence with the Code on biannual basis and the rendition shall be through the template provided in the Second Schedule to this Code.

## Chapter Eight

### Interpretation and Code Review

#### 8.1 Interpretation of Key Terms/Words

Below are definitions and interpretation of words and terms used or referred to in the Code:

*“Applications Service Provider”* - Any provider of a communications service through or via an application that relies on any licensed mobile communications network in Nigeria and as defined in Section 157 of the Act;

*“Communications Service”* - As defined in Section 157 to mean any service that provides means for, or facilitates any communication, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms;

*“content”* As defined in Section 157 of the Act to mean any sound; text, still picture, moving picture or other audiovisual representation, tactile representation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved or communicated electronically;

*“Content Applications Service”* As defined in Section 157 to mean an applications service which provides content;

*“Content filter”* - A tool that allows the user to control what can and what cannot be accessed online and/or on a network;

*“Customer/ Consumer”* - This is as defined in Section 157 of the Act;

*“Customer Information”* - Any record pertaining to a customer in paper, electronic, or any other form, that the Internet Access Service Provider collects and/or stores;

*“Data breach”* - An incident in which sensitive or confidential data is viewed, stolen or used by an unauthorized party;

*“Digital Service Provider”* - means any entity that provides any digital service through a digitalized or digitized medium that offers any form of communications service through or via a licensed mobile communications network based in Nigeria or to subscribers based in Nigeria;

*“Digital Communications Service”* means any form of communications service delivered either through a digitalized or digitized medium via the network of an Internet Access Service Provider licensed in Nigeria;

*“Harmful content”* - Any online content that is an image, video or words that causes offence, distress or harm.

*“Impacted entity”* – Any person or entity that is not a holder of an Individual licence of the Commission and provides any service that is within the purview of the Nigerian Communications Act 2003;

*“Individual Licence”* – As defined in Section 157 of the Act means a licence for a specified person to conduct a specified activity and may include conditions to which the conduct of that activity shall be subject;

*“Internet Access Service”* - A publicly available electronic communications service, irrespective of the network technology or terminal equipment used, that provides access to data communications to or from Network Termination Points with IP addresses that are assigned through delegation from the Internet Assigned Numbers Authority. This includes the provision of temporary access to the Internet;

*“Internet Access Service Provider”* - Any entity licensed by the Nigerian Communications Commission, engaged in the provision of an Internet Access Service, irrespective of the network technology or terminal equipment used, or the license held;

*“Law”* - As defined in the Interpretation Act CAP 123 LFN 2004, or any amendment thereto;

*“Lawful content”* - Any content that does not constitute unlawful content within the meaning of this Code;

*“Minor”* - Any individual under 18 years of age;

*“Misinformation”* - This refers to false or inaccurate information, especially that which is deliberately intended to deceive. Or incite the public

*“Non-harmful device”* - Any device that can be connected to a publicly available communications network, that conforms to industry standards and does not seriously degrade, obstruct or repeatedly interrupts the operations of the network;

*“Online and Digital Communications Platform”* - means any medium, process or method that permits or allows any communications services in part or as an enabling service, directly or through an intermediary;

*“Preferential data prioritization”* - The practice of granting preferential treatment to selected network data within the same service category based on the data’s origin, business agreements between Internet Access Service Providers and other entities, other commercial considerations or any other considerations that do not qualify as reasonable network management;

*“Parental Control Measures”* - Tools designed to enable parents and guardians monitor and control their children's online activities and use of mobile phones and other smart



devices;

*“Reasonable Network Management”* - Traffic Management Practices designed to enhance or protect quality of experience for consumers while complying with global standards for open internet access;

*“Relevant Organization”* – Any agency of government empowered by its establishing law with powers to request for takedowns of online content such as the Office of the National Security Advisor, Department of Security Services, Nigerian Police Force, Nigerian Copyright Commission, Nigerian Film Corporation or as may be so designated by the Commission from time to time.

*“Spam”* - Unsolicited and unwanted electronic messages typically sent to multiple recipients at once;

*“Spam filter”* - Any software or tool used for detecting spam in order to prevent them from reaching the user’s inbox;

*“Takedown Notice”* – A notice to withdraw or disable access to unlawful content issued by the Nigerian Communications Commission or any legal authority to Internet Access Service Providers or any entity that provides any form of service via or on a platform that relies on the Nigerian Communications network or its subscribers base;

*“Terminal equipment”* - As defined in Schedule 1, Part 1 (m) of the License granted by the Nigerian Communications Commission for the provision of Internet Services;

*“The Act”* - The Nigerian Communications Act 2003;

*“The Service”* - Internet Access Service;

*“Throttling”* - Network practice where data upload and download rates for specific services are intentionally restricted;

*“Unlawful content”* - Any content in violation of an existing law in Nigeria;

*“Usage Control Tool”* - Any software or tool that controls the usage of a terminal device, such as a tablet or mobile phone, by enforcing pre-set restrictions such as placing time limits on usage or prohibiting certain types of usage;

*“Usage Monitoring Tool”* - Any software or tool that can track or monitor the usage of a device it is installed on, including the user’s activity and location;

*“Vulnerable dependant”* - An individual who does not qualify as a minor but lacks the developmental and cognitive capabilities of a typical adult;

*“Zero rating”* - When an Internet Access Service Provider applies a price of zero to the

data traffic associated with a particular application or class of applications (and the data does not count towards any data cap in place on the internet access service).

## 8.2 Code Review

The Commission reserves the right to periodically review and update this Code of Practice in line with advances in technology and developments in the industry. This review shall be in line with the provisions of Section 72 of the Act and the procedure set therein.

## 8.3 Transition Provisions

All regulatory measures and decisions taken based on the Internet Code of Practice 2019 shall be construed as if undertaken under this Code and all subsisting actions and activities shall be guided by this Code.

Dated.....September, 2025

**Dr. Aminu Maida**

EVC/CEO Nigerian Communications Commission

### ***Explanatory Memorandum***

*This Code is a Guidelines issued in line with the powers of the Commission in Section 70 and its provisions apply to all licensees of the Commission, Impacted entities and all persons under the purview of the Nigerian Communications Act 2003 and its subsidiary legislations.*

## First Schedule

### Internet Access Service Provider Rendition Template

Name of Licensee			
Type of Licence			
Geographical Coverage Area			
Have you received any Takedown Request (s)			
Provide Details			
Outcome & Actions Taken			
Have you complied with relevant provisions of the Code			
Have you had any engagement with any Impacted Entity			
Provide Details			
Relevant Officer	Title/ Position	Reporting Period	Date/Signature

## Second Schedule

### Online Platform Rendition Template

Name of Impacted Entity			
Type of Service			
Geographical Coverage Area			
Have you received any Takedown Request (s)			
Provide Details			
Outcome & Actions Taken			
Have you adhered with relevant provisions of the Code			
Have you had any engagement with any Licensee of the Commission			
Provide Details			
Relevant Officer	Title/ Position	Reporting Period	Date/Signature

## Third Schedule

### Code Compliance Rendition Template

Name of Licensee/Impacted Entity			
Type of Licence/Service			
Geographical Coverage Area			
Is the Code aligned with your Community Rules/Guidelines?			
Provide Details			
Is there any part of the Code that conflicts with your processes?			
Have you complied with relevant provisions of the Code			
Are there compliance issues or non-compliance situation you want to self-report?			
Provide Details			
Relevant Officer	Title/ Position	Reporting Period	Date/Signature