



# Establishment of Internet Industry Code of Practice

Draft Code

June 2018

## Table of Contents

1	Preliminary.....	3
1.1	Preamble .....	3
1.2	Objectives of the Code .....	3
1.3	Application and Scope of the Code.....	3
1.4	Terminology and Interpretations.....	4
2	Right of Consumers to Open Internet Access.....	5
3	Standards for Open Internet Access.....	6
3.1	Transparency.....	6
3.2	No discrimination .....	6
3.3	No blocking .....	6
3.4	No throttling.....	6
3.5	No preferential data prioritisation .....	6
3.6	Zero-Rating.....	6
3.7	Acceptable Traffic Management Practices .....	7
4	Privacy and Data Protection Obligations.....	7
4.1	Compliance with Part VI of Schedule 1 of the Consumer Code of Practice Regulations 2007 .....	7
4.2	Data Security .....	7
4.3	Data Breach Notifications.....	8
5	Online Protection of Minors and other Vulnerable Dependants .....	8
5.1	Incorporation of Child Online Protection Policies into Terms and Conditions of Service .	8
5.2	Reporting Mechanism for Child Sex Abuse Content .....	8
5.3	Blocking of Access to Child Sexual Abuse Content.....	8
5.4	Parental Control Measures.....	8
5.5	Education of Parents, Guardians, and Minors .....	9

6	Safeguards against Unsolicited Internet Communications .....	9
6.1	Incorporation of Anti-Spam Policies into Terms and Conditions of Service.....	9
6.2	Spam Filters.....	10
7	Obligations pertaining to unlawful Content.....	10
7.1	No Monitoring Obligation .....	10
7.2	Procedure for Reporting Unlawful Content.....	10
7.3	Takedown Notice.....	10
7.4	Collaboration with Law Enforcement on unlawful Content.....	10
8	Obligations of Internet Access Service Providers under existing laws.....	11
9	Monitoring and Enforcement.....	11
9.1	The Commission.....	11
9.2	Consumer Web Portal.....	11
10	Code Review.....	11

# **1 Preliminary**

## **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.

An Open Internet is key for successfully driving innovation, but there are several factors to consider in the promotion of a truly open internet, such as online child protection, privacy and data protection, objectionable content, unsolicited communications, and traffic management practices that are considered necessary in order to maintain network efficiency.

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, set out to establish this Internet Code of Practice to clearly define the rights and obligations of Internet Access Service Providers with regard to the issues therein.

The establishment and enforcement of the Code is envisioned as a co-regulatory effort between the Commission and industry stakeholders, hence the extensive public consultation and incorporation of stakeholder feedback into the final document.

## **1.2 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) Establish best practices for Internet Governance in Nigeria, in line with emerging issues and global trends.

## **1.3 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.

#### 1.4 Terminology and Interpretations

The interpretations of terms used within the Code are as follows:

<b>Communications Service</b>	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.
<b>Content Filter</b>	A tool that allows the user to control what can and what cannot be accessed online and/or on a network.
<b>Customer/Consumer</b>	As defined in Section 157 of the Nigerian Communications Act, 2003.
<b>Customer Information</b>	Any record pertaining to a customer in paper, electronic, or any other form, that the Internet Access Service Provider collects and/or stores.
<b>Data Breach</b>	An incident in which sensitive or confidential data is viewed, stolen or used by an unauthorized party.
<b>Internet Access Service</b>	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.
<b>Internet Access Service Provider</b>	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.
<b>Law</b>	As defined in the Interpretation Act CAP 123 LFN 2004, or any amendment thereto.
<b>Lawful content</b>	Any content that does not constitute unlawful content within the meaning of this Code.
<b>Minor</b>	Any individual under 18 years of age.
<b>Preferential data prioritisation</b>	The practice of granting preferential treatment to selected network data within the same service category based on the data's origin, business agreements between IASPs and other entities, other commercial considerations, or any other considerations that do not qualify as reasonable network management.
<b>Parental Control Measures</b>	Tools designed to enable parents and guardians monitor and control their children's online activities and use of mobile phones and other smart devices.

<b>Reasonable Network Management</b>	Traffic Management Practices designed to enhance or protect quality of experience for consumers while complying with global standards for open internet access.
<b>Spam</b>	Unsolicited and unwanted electronic messages typically sent to multiple recipients at once.
<b>Spam Filter</b>	Any software or tool used for detecting spam in order to prevent them from reaching the user's inbox.
<b>Takedown notice</b>	A notice issued to IASPs by the Nigerian Communications Commission or other legal authority to withdraw or disable access to unlawful content.
<b>Terminal equipment</b>	As defined in Schedule 1, Part 1 (m) of the License granted by the Nigerian Communications Commission for the provision of Internet Services.
<b>The Act</b>	The Nigerian Communications Act 2003.
<b>The Service</b>	Internet Access Service.
<b>Throttling</b>	Network practice where data upload and download rates for specific services are intentionally restricted.
<b>Unlawful content</b>	Any content in violation of an existing law in Nigeria.
<b>Usage Control Tool</b>	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.
<b>Usage Monitoring Tool</b>	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.
<b>Vulnerable Dependant</b>	An individual who does not qualify as a minor but lacks the developmental and cognitive capabilities of a typical adult.
<b>Zero-rating</b>	When an IASP 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).

## 2 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.

### **3 Standards for Open Internet Access**

#### **3.1 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.

#### **3.2 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.

#### **3.3 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.

#### **3.4 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.

#### **3.5 No preferential data prioritisation**

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

#### **3.6 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, and with the approval of the Commission.

### **3.7 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.

## **4 Privacy and Data Protection Obligations**

### **4.1 Compliance with Part VI of Schedule 1 of the Consumer Code of Practice Regulations 2007**

An Internet Access Service Provider shall comply with the provisions of Part VI of Schedule 1 of the Consumer Code of Practice Regulations 2007 or as may be amended by the Nigerian Communications Commission, on Protection of Consumer Information, in addition to the provisions stated hereunder.

### **4.2 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.

### 4.3 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 72 hours of its occurrence, by email and text message.
- b) *Notification of the Commission*: An Internet Access Service Provider shall formally notify the Commission of any breach no later than 72 hours after the Internet Access Service Provider reasonably determines that a breach has occurred.

## 5 Online Protection of Minors and other Vulnerable Dependants

### 5.1 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 complies with the Cybercrime Act 2015, 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.

### 5.2 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.

### 5.3 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.

### 5.4 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 5.4 (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.
- 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.

## **5.5 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:
  - 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, 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.

## **6 Safeguards against Unsolicited Internet Communications**

### **6.1 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.

## **6.2 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 will 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 6.2 (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.

## **7 Obligations pertaining to unlawful Content**

### **7.1 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 under any obligation to seek facts or circumstances indicating unlawful activity, except when acting under instruction from the Commission or relevant law enforcement agency.

### **7.2 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.

### **7.3 Takedown Notice**

- a) Upon determination by the Commission that the content reported under Paragraph 7 (2) above is indeed unlawful, the Commission shall issue a takedown notice to all IASPs to deny or disable access to the content. The IASP shall be expected to comply with such takedown notice within 24 hours of receipt of the notice.
- b) A person who is aggrieved or whose interest is adversely affected by any takedown notice issued by the Commission pursuant to Paragraph 7.3 (a) above may appeal the decision in accordance with the provision of Chapter V, Part X of the Act.

### **7.4 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.

## **8 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 2015, terms and conditions of their license, and all applicable Regulations and Guidelines.

## **9 Monitoring and Enforcement**

### **9.1 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 indicate its subsequent level of compliance with the Code in a report submitted to the Commission within fourteen days.
- b) The monitoring and enforcement of the Code will be exercised in accordance with the Nigerian Communications (Enforcement Processes, etc.) Regulations 2005. With respect to any penalties for contravention of applicable provisions, the Commission will be guided by the considerations set out in the Regulations.

### **9.2 Consumer Web Portal**

- a) The NCC Consumer Web Portal will be updated to accept complaints from consumers about non-compliance with the Code from their Internet Access Service Provider.
- b) Complaints submitted to the portal will be reasonably investigated by the Commission in accordance with its complaints adjudicatory processes.

## **10 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.