THE AFRICAN ADVANCED LEVEL TELECOMMUNICATIONS INSTITUTE (AFRALTI)



BRIEF REPORT

ON

HUMAN CAPACITY DEVELOPMENT FOR THE CHILD ONLINE PROTECTION (COP) PROGRAMME IN KENYA

24TH **OCTOBER 2021**

Contents

1.	BACKGROUND	3
2.	STRUCTURE OF THE WORKSHOP	4
3.	PARTICIPATION	4
4.	TRAINING METHODOLOGY	4
	I. In- person Training (face to face Training)	4
	II. ONLINE TRAINING	5
	III. SYSTEM REQUIREMENTS FOR THE ONLINE STUDENTS' COMPUTERS	5
5.	PROGRAMME OUTLINE	6
6.	DELIVERY MODE	7
7.	LEARNING OUTCOMES	7
8.	COURSE TOPICS	8
9.	Executive Summary	13
(Child Online Protection Training 2019 (Year 1)	13
(Child Online Protection Training Programme 2020 (Year 2)	13
(Child Online Protection 2021 (Year 3)	14
10	. Summary Table	15
11.	. Sample Training Program	15
12.	. DATA PROTECTION	17
13.	CERTIFICATION	17
,	Annex 1: Group picture –OFFICIAL COP OPENING CEREMONY	17
,	Annex 2: Group picture – In- Person on going session	17
,	Annex 3: Group picture – OPENING SPEECH BY HEAD OF TRAINING AT AFRALTI	18
,	Annex 4: Group picture – COP COHORT 1 YEAR 2 January 2020	19
,	Annex 5: Group picture – COP VIRTUAL Training	19
,	Annex 6: Group picture – VIRTUAL Training May 2021 cohort	20
,	Annex 7: Group picture – VIRTUAL Training June 2021 cohort	20
,	Annex 8: Group picture – VIRTUAL Training August 2021 cohort	21
	Annex 9: COP Graduation day for In-person class	21

1. BACKGROUND

With children making up an estimated one third of internet users worldwide, living in the 'digital age' can have important implications for children's (Child safety online, Technical report 2012). Studies have shown that 90 percent of the children surveyed used the internet, with 50 percent spending between one to two hours online every day. There is increased tendency by public internet access points to admit unaccompanied minors and with no parental consent. Additionally, these points often fail to restrict prohibited online sites from access by children.

Kenyan children are faced with enormous challenges with regards to access and use of the internet with studies on child safety and security indicating that a quarter of Kenyan children with internet access are exposed to sexually explicit materials with only 24 percent of the children reporting such incidences.

The Digital Literacy Program and the Computer and Cybercrime Bills recently implemented by government is a welcome initiative, but also presents a new challenge as more Kenyan children being enabled to access the internet. Safeguards therefore have to be put in place to educate stake holders on the issues that could arise and how to protect the children from online harm.

AFRALTI proposed a partnership with Communications Authority of Kenya (CA) to deliver training to high level, high impacts groups within our society in a bid to create a healthy online experience for our children and youth over a three-year initial program. This is envisaged to be a long-term partnership that will involve building the capacity of key stakeholders to tackle issues arising out of children's online presence.

As result of this gap, AFRALTI proposes to focus on the following areas:

- (a) What is Child On-line Protection?
- (b) Child Online Protection in light of the Computer and Cybercrimes Bill
- (c) Types of online crimes
- (d) Guidelines to prevent online abuse
- (e) Safe online tips for parents / caregivers/ teachers and Guardians

2. STRUCTURE OF THE WORKSHOP

The training workshop was carried out as a multi stakeholder training. To create value addition and have an impactful program, AFRALTI partnered with various organizations to deliver the training.

A pool of experts from the following organizations have supported us to deliver the Child Online Protection (COP) programme.

Organization	Topics				
FACEBOOK / GSMA	 Combating Child Exploitation Child Online Safety and Well-being 				
Kenya Law Reforms Commission (KLRC)	Cyber Laws				
DCI – Kenya	Law enforcement				
ISOC	Safer working practices for those working or volunteering with children				
Cyber Speak Kenya	Cybersecurity threats				
National Ke-ICRT	Case Scenarios				
AFRALTI	CSCU, Hands-on Cyber security				
Childline Kenya	Case scenarios				
Eveminet	Safety online culture.				
Internet Watch Foundation (IWF)	Online reporting Mechanism				
International Center of Missing and Exploited Children (ICMEC)	International investigative cases& Statistics				

3. PARTICIPATION

The participants for the training program came from various organizations and institutions both governmental and non-governmental.

4. TRAINING METHODOLOGY

I. In- Person Training (face to face Training)

To facilitate the most effective learning process, the training methodology adopted by AFRALTI utilizes a blended learning method involving powerful hands-on instructor led sessions. Instructor-Led Trainings allows AFRALTI to build upon learned knowledge by giving learners a chance to put knowledge and skills into practice through classroom activities. Hands-on training (as experiential

learning) will be incorporated in this training this will make it effective for learning software applications, procedures and devices, and also helps instructors immediately determine whether a student has adequately learned a new skill or process.

Venue of the In- person Training has been at AFRALTI main campus.

II. ONLINE TRAINING

A mixture of virtual online training and self-paced training.

a) Interactive Live Classroom Sessions

Live interactive classroom sessions has been on ZOOM. ZOOM has enabled participants/students and Instructors to engage in video conferencing, send instant messages and share files with the participants during the training sessions. The tool is available on mobile devices, computers or tablets.

b) AFRALTI Online Learning Management Platform

This training will be delivered on AFRALTI online learning management platform built on Moodle. Moodle is one of the best learning platforms designed to provide educators, administrators and learners with a single robust, secure and integrated system to create personalized learning environments.

c) Timings.

Total Class duration is 40 hours.

- 16 hours for Virtual Instructor led training
- 24 hours for online self-paced training
- Virtual Instructor led classes have been conducted on weekdays (Tuesday and Thursday, 11am-1pm) for 4 weeks (16 Hours).
- Participants were required to do **two hours** of self-paced study daily and take associated assessments from the e-learning platform to test their knowledge.

III. SYSTEM REQUIREMENTS FOR THE ONLINE STUDENTS' COMPUTERS

- Windows 7 desktop Systems or Mac OS X 10.10
- RAM of 8GB
- Core i5 processor

We recommend a speed of 5 Mbps for the interactive sessions, access to AFRALTI e-learning platform and for other learning activities

5. PROGRAMME OUTLINE

Title: Child Online Protection (COP)

OVERVIEW:

The explosion of information and communication technology has created unprecedented opportunities for children and young people to communicate, connect, share, learn, access information and express their opinions on matters that affect their lives and their communities. But the wider and more easily available access to the Internet and mobile technology also poses significant challenges to children's safety – both online and offline.

This programme targeting primary and secondary school teachers will equip the learners with essential skill necessary to protect the children when online.

PRE-REQUISITE:

Basic knowledge in computer application.

TARGET AUDIENCE:

While this course is specifically designed for primary and secondary school teachers, it can also benefit anyone using computers/smart devices, the Internet and online services for business or personal use.

PAIN POINT

With advancement of Technology, children are exposed to devices connected to the Internet and their Safety Online is not guaranteed. This course will prepare teachers to take their specific roles on how to protect children online.

WORKSHOP OBJECTIVES:

- To practically learn the fundamental cyber security skills
- To explain the various laws related to online child exploitation
- To learn the countermeasures to take after suspected child exploitation incident
- To address the capacity building necessary for a full-proof child online protection society
- To discuss national policies and frameworks to ensure child online safety
- To discuss existing international collaborations that to mitigate online child exploitation across the globe

VALUE PROPOSITION

Children are a vulnerable group and there have been many cases of children unknowingly getting into dangerous situations that sometimes have detrimental effects to them. Protecting children online is a global problem that requires concerted efforts of parents, guardians, the government and organizations that focus on children, among others.

The launch of the Digital Literacy Program has increased the number of children accessing technology and as such the initiative will ensure safeguards are put in place for their proper use. In addition, the reports generated from this initiative will provide sufficient information to support the policy and legal frameworks for child online protection to be established by the relevant entities.

In line with CA mandate as the ICT regulator, this programme responds to the need of protecting consumers of ICT services with children being among the most vulnerable.

6. DELIVERY MODE

Duration: 5 days for In- person training and 4 weeks for online training

Time: 8.00 am – 5.00 pm for In-person Training

Virtual training was conducted every Tuesday and Thursdays at 11:00AM to 01:00PM

Venue: AFRALTI for in- person training and Online for Virtual Instructor led Training (VILT)

7. LEARNING OUTCOMES

- Understand to create School ICT Policy and guidelines
- Learn how to use ICT devices or machines safely
- Learn their rights and responsibilities when using ICT devices and accessing the Internet
- Safeguarding child's digital footprint
- How to deal with offensive, inappropriate and illegal content
- Setting up and securing online conferencing platforms on ZOOM, Google, Skype, local platforms etc.
- Understand the need and importance of data security.
- Implement Operating System security measures on their computers.
- Understand Malware and its symptoms.
- Make an informed decision about choosing the antivirus which is most relevant to their needs.
- Understand the risks associated with different online activities.
- Understand why and how to secure web browsers.
- Identify safe websites.
- Safeguard against the threats associated with online social networking.
- Understand how to make their social networking accounts secure.
- Understand the threats associated with email communications and how to safeguard against them.
- Understand the threats to mobile devices and how to safeguard against them.
- Understand the threats associated with cloud accounts and how to safeguard against them.
- Make an informed decision about a cloud service provider which fulfils their requirements.

- Understand the various types of networks and the threats associated with them.
- Configure a home network.
- Make their networks secure.
- Understand the threats to data and the need for data backups.
- Backup and restore data on their computers.
- Destroy data permanently.

8. COURSE TOPICS

1. School ICT Policy and guidelines

- Establishing the various virtual training platforms, their functionality, benefits and requirements (E.g. Teachers educating on Zoom, Skype in the classroom, Google for education, intel education- teaching tools and resources e.t.c).
- Establish and document resources and tools required by school, teachers and children and how they can be used.
- Secure Internet devices (Parental Guidance (PG) configurations, passwords, antivirus, firewalls etc.).
- Taking and storing images of children and content used and accessed by children.
- Technical knowledge on information security management.

2. Safe use of ICT devices or machines

- Children's rights and responsibilities when using ICT devices and accessing the internet including broadcasting devices
- Developing child online safety guidelines for school
- Productive use of Internet
- Online safety tools have for machines/devices

3. Children's rights and responsibilities when using ICT devices and accessing the Internet

- How to communicate and socialize professionally with peers and adults in appropriate manner and in line with the national goals for education
- Acquire skills on how to protect themselves from online risks and vulnerabilities e.g. avoid certain websites, not sharing passwords, using strong passwords, not divulging private information etc.
- How to react when they encounter risks and vulnerabilities online (cyberbullies, perpetrators, addiction, online child sexual exploitation etc.)
- Understand implication of posting photos online and use of webcams
- How to say no especially to strangers and to inappropriate requests for information and images
- Avoid meeting people they first have met online
- Avoid engaging and expressing emotions to strangers online
- Online Etiquette (netiquette)
- Understand that not everyone online is who they claim to be
- Seek adults/educator's guidance when child want to purchase something online

- How to share online experiences
- How to make their online experience better and safer

4. Safeguarding Child's digital footprint

- Acquire skills on how to protect themselves from online risks and vulnerabilities e.g. avoid certain websites, not sharing passwords, using strong passwords, not divulging private information etc.
- Define information that should be kept private and not shared online
- Developing and using strong passwords
- Define what can be shared and what cannot be shared online

5. Dealing with offensive, inappropriate and illegal content

- Disclosing online risks and vulnerabilities encountered by themselves and peers
- Handling situation when children encounter risks and vulnerabilities online (cyberbullies, perpetrators, addiction, online child sexual exploitation etc.)
- Need for Support and empathy from peers who have been exposed to risks and vulnerabilities
- Importance of authoritative information to make better use decisions
- Guidance from adults and educators on best use on ICT's and how to access safe and child friendly sites.
- Reporting online cases and incidents

6. Securing online conferencing platforms on ZOOM, Google, Skype, local platforms etc.

- Use of strong passwords
- Control file sharing in chat to keep sensitive data safe
- Control conference/call recordings
- Use of encryption

7. Securing Operating Systems

- Guidelines To Secure Windows
- Lock the System When Not In Use
- Create a User Account Password
- Change a User Account Password
- Disable the Guest Account
- Lock Out Unwanted Guests
- Rename The Administrator Account
- Disable Jump Lists
- Enable Software Updates
- Enable and Configure Windows Firewall
- Turn on Windows Defender
- Enable bitlocker
- Windows Encrypting File System
- How to Decrypt a File Using EFS
- Disabling Unnecessary Services

- Killing Unwanted Processes
- How To Hide Files and Folder
- Disable Simple File Sharing
- Raise The UAC Slide Bar

8. Malware and Antiviruses

- Symptoms Of Malware Infection
- Antivirus
- How Does Antivirus Work
- How to Choose The Right Antivirus Software
- Configuring and Using Antivirus Software
- Kaspersky PURE 3.0
- Avast Antivirus
- How To Test If an Antivirus is Working

9. Internet Security

- Securing the Web Browser
- Browser Features and Their Risks
- Identify a Secure Website
- Understanding IM Security
- Instant Messaging Security Issues
- Instant Messaging Security Measures
- Understanding Child Online Safety
- Risks Involved Online
- Determining if Children are at Risk Online
- Protecting Children from Online Threats
- Encourage Children to Report
- How to Report a Crime
- Actions To Take When a Child Becomes a Victim of Online Abuse
- Safe Browsers for Children

10. Security On Social Networking Sites

- Top Social Networking Sites
- Creating a Profile
- Information Available on Social Networking Sites
- Security Risks Associated with Social Networking Sites
- Geotagging
- Facebook Security Settings
- Facebook Privacy and Security Settings
- Profile Settings
- Privacy Settings for Applications
- Settings to Block Users
- Recommended Actions for Facebook Search Settings
- Twitter Security Settings

11. Securing Email Communications

Email Clients

- Email Service Providers
- Email Security
- Malicious Email Attachments
- Malicious User Misdirection
- Email Security Threats: Phishing
- Email Security Threats: Hoax Mail
- Nigerian Scam
- Spamming
- Anti-Spamming Tool: SPAMfighter
- Understanding Various Email Security Procedures
- Create and Use Strong Passwords
- Disable Keep Me Signed In/Stay Signed In Functions
- Provide Recovery Email Address for Mail Recovery
- Use HTTPS Enabled Email Service Provider
- Turn Off the Preview Feature
- Avoid Unwanted Emails Using Filters
- Scan Email Attachments for Malware
- Check for Last Account Activity
- Digitally Sign Your Emails
- Encrypt Your Mails
- Email Security Tools

12. Securing Mobile Devices

- Securing Mobile Devices
- Mobile Operating Systems
- Importance of IMEI Number
- Mobile Malware
- Mobile Application Vulnerabilities
- Threats to Bluetooth Devices
- Updating Mobile Operating Systems
- Updating Applications in Android Devices
- Install Mobile Phone Antivirus
- Securing Bluetooth Connectivity
- Securing Wi-Fi Connectivity
- Mobile Device Encryption
- Avoiding Mobile Device Theft
- Understanding How to Secure Android Devices
- Android: Setting Screen Lock
- Android: Setting SIM Lock
- Android: Data Backup
- Android: Encrypting the Phone
- Android: Android Device Manager
- Mobile Security Tools

13. Securing The Cloud

- Cloud Services
- Data Breach
- Data Loss
- Account Hacking

- Disgruntled Insider
- Technology Loopholes
- Shared Space
- Safeguarding Against Cloud Security Threats
- Back Up Data
- Update Backups Regularly
- Create Strong Passwords
- Choose Two Step Authentication
- Encrypt
- Have a Disciplined Online Behavior
- Avoid Storing Sensitive Data on Cloud
- Cloud Privacy Issues
- Encrypt data
- Read Terms and Conditions Carefully
- Avoid the Share Feature on Cloud
- Avoid Storing Sensitive Data on Cloud

14. Securing Network Connections

- School Networks
- Home Network
- Setting Up a Wireless Network in Windows
- Common Threats to Wireless Network
- Securing Wireless Network
- Measures to Secure Network Connections: Firewall, Antivirus, Encryption

15. Data Security

- Data Backup
- Backup Types: Online, Full, Incremental,
- Windows Backup and Restore Procedures
- Secure Data Destruction
- The Need Destroy Data Permanently
- Deletion Vs. Permanent Destruction
- Ways to Permanently Destroying Data

16. Acceptable Use Policy

- Safeguarding and Child Protection
- Anti-bullying & Online harassment
- Communication
- Risk Assessment
- Code of conduct ~ staff
- Confidentiality agreement
- Data protection & Management
- Incident handling and reporting
- Digital Footprint
- Online Participation Consent (Student and Parent/guardian)
- Protection from Sexual Exploitation & Abuse
- Standard Operating Procedures Virtual Classroom setup
- Security setup on Learning platforms
- Guidelines for reporting 16. Guidelines for safeguarding staff.

9. Executive Summary

The table below shows the number of participants trained till so far through Communications Authority of Kenya (CA) sponsorship.

Table 1: Number of Participants in the last 6 years

Year	No. of Participants Trained	No. of Cohorts
2019	36	1
2020	60	2
2021	332	6
Total	428	9

Child Online Protection Training 2019 (Year 1)

Communications Authority of Kenya (CA) sponsored the Child online Protection, the training programme was conducted at AFRALTI.

A total of 36 participants were trained in the out 0f 50 registered participants.

The 5 days training was held in the form of a full day training (08:00 - 16:30). The training approach was instructor led training in form of an interactive workshop with group works, slides and video presentations.

The training had participants from different organizations with different professions but with a common interest in Online Child Protection. The participants were from Kenya and one from Malawi (see attendance list attached).

The facilitators were drawn from different organization as follows

- GSMA (UK & Kenya offices (2)
- Facebook (UK) (1)
- Kenya Law Reforms Commission (KLRC) (2)
- Directorate of Criminal Investigations (DCI)- Cyber Security department and Children Protection Department (2).
- AFRALTI (2)

Child Online Protection Training Programme 2020 (Year 2)

AFRALTI working jointly with Communications Authority of Kenya (CA) sponsored the Child online Protection, the training programme was conducted at AFRALTI.

A total of 60 participants were trained in the out 0f 120 registered participant the training was held in 2 cohorts January – 25 participants and 35 participants in February 2020.

The facilitators were drawn from different organization as follows

- GSMA (UK & Kenya offices (2)
- Kenya Law Reforms Commission (KLRC) (2)
- Directorate of Criminal Investigations (DCI)- Cyber Security department and Children Protection Department (2).
- Internet Society of Kenya
- AFRALTI (2)

The training was put on hold with the occurrence of COVID-19 pandemic where all learning institutions were closed by the head of State to curb the spread of the disease.

Child Online Protection 2021 (Year 3)

Communications Authority of Kenya requested AFRALTI to continue with the training program but virtually. A total of 332 participants were trained in the 86 cohorts. The trainings were all virtually delivered.

The facilitators Included:

- 1) AFRALTI
- 2) Terres Des Hommes Netherlands
- 3) Kenya Law Reforms (KLR)
- 4) Directorate of Criminal Investigation (DCI)
- 5) University of Pretoria
- 6) Internet Watch Foundation (IWF)
- 7) International Center for Missing and Exploited Children (ICMEC)
- 8) Cyber Speak Africa
- 9) GSMA

10. Summary Table

		PARTICIPATION					
Month	COHORT	Confirmed	Trained Registered on Moodle	Achieved Pass mark	Did not achieve pass mark	Registered but did not attempt course	Total Trained
	In- Person Training						
Nov 2019	Cohort 1 year 1	50					36
Jan 2020	Cohort 1 year 1	60					25
Feb 2020	Cohort 1 year 1	60					35
	Virtual Instructor Led Training						
Feb 2021	Cohort 1 year 2	50	40	33	6	1	39
Mar 2021	Cohort 2 year 2	50	46	43	1	2	44
Apr 2021	Cohort 3 year 2	70	65	55	3	7	58
May 2021	Cohort 4 year 2	80	76	64	1	11	65
Jun 2021	Cohort 5 year 2	75	73	67	1	5	68
Aug 2021	Cohort 1 year 3	70	63	57	1	5	58
Total	8						428

11. Sample Training Program

COP VIRTUAL TRAINING PROGRAMME					
DAY	SPEAKER/PLATFORM	TOPIC	TIME		
DAY 1: MONDAY	Athena Morgan (AFRALTI)	Tutorial on AFRALTI Online Academy / Moodle Learning Platform	11:00am- 01:00pm		
DAY 2: TUESDAY	Anita Natwati & Athena Morgan to work with CA Team Zoe Colpert (IWF) / ZOOM	 ✓ Online Child cases reporting mechanism ✓ Collaboration with other organizations 	11:00am-12:00am 12:00am- 01:00pm		

		 ✓ Hands on Skills Password Protecting various gadgets. 	
DAY 3: WEDNESDAY	AFRALTI Online Academy	 ✓ Self-paced training ✓ Quizzes and discussions 	Open
DAY 4: THURSDAY	Athena Morgan (AFRALTI) ZOOM	 ✓ Digital Identity/ Responsible digital Citizenship ✓ Online Crimes Internet Addiction 	11:00am- 01:00pm
DAY5 & 6: FRIDAY & MONDAY	AFRALTI Online Academy	✓ Self-paced training✓ Quizzes and Discussions	Open
DAY 7: TUESDAY	Felix Ngugi (CyberSpeak PLC) /ZOOM	✓ Emerging Issues on WWW✓ Online Environment- Appropriate/ Inappropriate	11:00am- 01:00pm
DAY 8: WEDNESDAY	AFRALTI Online Academy	✓ Self-paced Training✓ Quizzes and discussions	Open
DAY9: THURSDAY	Wilson Macharia /ZOOM	 ✓ The Online life of a Child with Disabilities (CWDs) ✓ Online Abuse of CWDs ✓ Importance of Internet and Tech for CWDs 	11:00am- 01:00pm
DAY 10 & 11: FRIDAY, & MONDAY	AFRALTI Online Academy	✓ Self-paced training✓ Quizzes and Discussions	Open
DAY 12: TUESDAY	Steve Gachogu (AFRALTI) Catherine Masinde (AFRALTI) /ZOOM	✓ Cybersecurity✓ Network Security	11:00am- 01:30pm
DAY 13: WEDNESDAY	AFRALTI Online Academy	✓ Self-paced training✓ Quizzes and Discussions	Open
DAY 14: THURSDAY	Irene Kabua & Evelyne Kogi (Kenya Law Reforms) /ZOOM	✓ Children's Act✓ Constitution &International Laws	11:00am- 01:30pm
DAY 15 & 16: FRIDAY & MONDAY	AFRALTI Online Academy	✓ Self-paced training✓ Quizzes and Discussions	Open
DAY 17: TUESDAY	Lawrence Agolla (DCI) /ZOOM	✓ Law enforcement in Children cases ○ Case Scenarios	11:00am- 01:00pm
DAY 18 :WEDNESDAY	AFRALTI Online Academy	✓ Self-paced training✓ Quizzes and Discussions	Open
DAY 19: THURSDAY	ICMEC / ZOOM	 ✓ Online Solicitation ✓ Exploitation of Missing Children ✓ Cases and Statistics 	11:00am- 01:00pm
DAY 20: FRIDAY	AFRALTI Online Academy	✓ QuizzesParticipants' Feedback	Open
DAY 21: THURSDAY	Closing Ceremony	✓ Opening Remarks	11:00am- 12:00pm

AFRALTI/ CA Team.

- ✓ Communication Authority of Kenya (CA)
- ✓ Closing Remarks J. P. Mwakijele (AFRALTI)
- ✓ List of Qualified participants, Instructions on certificate pick-up.
- ✓ Closing Prayer

12. DATA PROTECTION

The data that collected is treated by AFRALTI with privacy as stipulated by Kenya Data Protection Act 2019.

13. CERTIFICATION

Participants who successfully complete this training will be awarded AFRALTI Certificate of Completion.

Annex 1: Group picture -OFFICIAL COP OPENING CEREMONY



Annex 2: Group picture – In- Person on going session





Annex 3: Group picture – OPENING SPEECH BY HEAD OF TRAINING AT AFRALTI



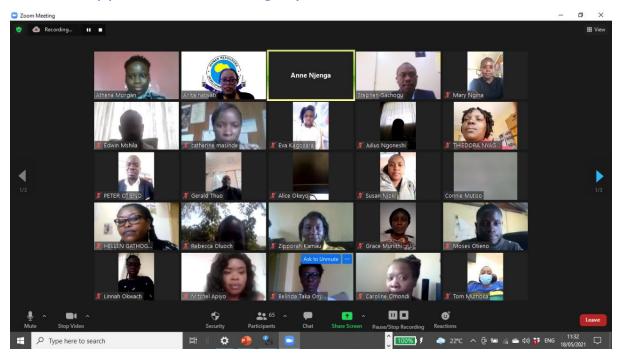
Annex 4: Group picture – COP COHORT 1 YEAR 2 January 2020



Annex 5: Group picture – COP VIRTUAL Training



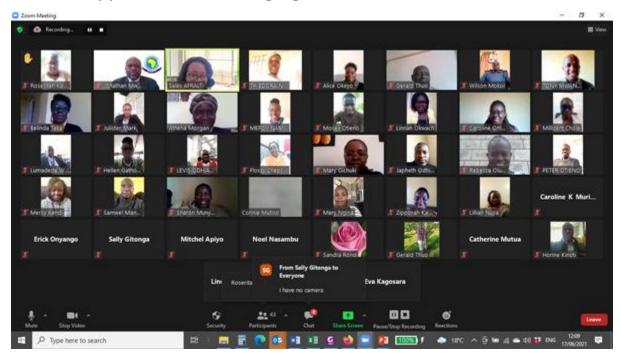
Annex 6: Group picture – VIRTUAL Training May 2021 cohort



Annex 7: Group picture – VIRTUAL Training June 2021 cohort



Annex 8: Group picture – VIRTUAL Training August 2021 cohort



Annex 9: COP Graduation day for In-person class



For More Information contact us:

Main Campus: Waiyaki Way, Adjacent to the Communications Authority of Kenya (CA) Nairobi, Kenya.

Town Campus: Kimathi House, 3rd floor 305, Nairobi CBD, +254 776 231 14l

Mailing Address: PO. Box 58902-00200, City Square, Nairobi, Kenya.

Telephone:

+254 710 207061, +254 20 2655011, +254 20 2655012

+254 20 4440633 -Technology Dept (Cisco & DT-MIS)

+254 0202462160/61. Business Development

Email: training@afralti.org , info@afralti.org

Website: http://www.afralti.org

FB: <u>@AFRALTI</u> Twitter: <u>@AFRALTI</u> Instagram: <u>afralti_org</u>

<u>LinkedIn: The African Advanced Level Telecommunications Institute</u>

YouTube: AFRALTI