DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

PAPUA NEW GUINEA SOCIAL MEDIA POLICY

2025

GLOSSARY

DEFINITIONS

Abuse of Platforms – is the misuse of online platforms for harmful, unethical, or illegal activities.
Accessibility Rate – refers to the proportion or percentage of people who have access to a service or technology.
Cyber-Attack – refers to the deployment of malicious software into an electronic system or device, data and infrastructure for the purpose of altering and causing harm or disruption.
Cyber-Bullying – Use of electronic systems and devices or digital platforms such as social media, messaging apps, or online forums to threaten, intimidate, demean, ridicule, stalk and cause emotional distress.
Child Protection – refers to safeguarding children from abuse, neglect, exploitation, and harm, ensuring their safety, well-being, and development.
Children Under the Age of 18 – Individuals legally considered minors and in need of special protection.
Content Filtering – Mechanisms to remove harmful, false, or inappropriate material from social media.
Content Regulation – refers to the policies and laws that govern the type of material that can be published, shared, or broadcast, particularly on media platforms and the internet.
Cyber Crime – offenses committed through the use of information and communication technology (computers, networks, or the internet).
Cyber Harassment – The act of harassing individuals through digital means such as social media or messaging platforms.
Cyber Hygiene – Practices that ensure safe and secure use of digital systems and online spaces.
Cyber Threats – Potential malicious activities targeting digital systems, data, or infrastructure.
Cyber Security – is the practice of protecting computer systems, networks, and digital data from unauthorized access, theft, damage, or disruption.
Data Security – Protection of digital information from unauthorized access, corruption, or theft.
Decency – Encouraging users to exhibit morally acceptable behavior online.
Digital Platforms – are online systems or frameworks that facilitate interactions, transactions, or the exchange of information between users, for example: social media platform.
Digital Platform Owners – Entities that develop and manage online platforms.
Digital Skills – Abilities related to effectively using digital tools, platforms, or technologies.
Digital Tools – Software, platforms, or devices used for communication, collaboration, or productivity in the digital realm.
Disinformation – is the deliberate creation and dissemination of false or misleading information with the intent to deceive or manipulate audience.
e-Safety – refers to the practice of protecting individuals, particularly children and young people, from online risks such as cyberbully, identity theft, and exposure to inappropriate content.

Fact Checking – refers to investigating an issue in order to verify the facts. The investigation is conducted to confirm the accuracy (sources: primary or secondary) of information and statements made by individuals, group or organization.
Factual – Requiring users to disseminate truthful and accurate information.
Fake news – refers to false information reported or circulated as "true", using various communication platforms such as social media to cause confusion and mislead audiences.
Harmful Content – Material online that may negatively impact mental, emotional, or social well-being.
Information Dissemination – The distribution and sharing of information to a wide audience.
Internet – is a global network of interconnected computers and servers that allows users to share and access information, communicate, and interact through websites, applications, and services.
Internet Service Providers (ISPs) - Companies that provide internet access to individuals or organizations.
Law Enforcement – Governmental agencies or activities aimed at maintaining law and order. Legal-Mandating users to follow applicable laws and regulations in their online activities.
Misinformation and Disinformation Management – Policies to prevent the spread of false, defamatory, or misleading information online.
Misinformation – refers to false or inaccurate information that is spread without the intent to deceive.
National Security – Policies aimed at protecting citizens from cyber threats, identity theft, and breaches of sensitive information.
Online – refers to being connected to or available through the internet, enabling access to digital services, platforms, and communication tools.
Online Abuse – Harmful or offensive behavior directed at individuals through digital platforms.
Online Harassment – Unwanted, harmful, or abusive behavior targeted at individuals through digital platforms.
Online Platforms – are digital spaces or systems accessible via the internet that enable users to interact, communicate, share content, or conduct transactions. Examples include social media sites.
Platform Accountability – The responsibility of social media platforms to align with laws, ensure data transparency, and support ethical practices.
Platforms – Online services or applications such as Facebook, Instagram, TikTok, and LinkedIn that facilitate user interaction.
Privacy - users to understand and utilize privacy settings to protect personal information.
Privacy Breaches – Incidents where unauthorized access or exposure of personal or sensitive information occurs.
Regulate – To control or manage activities through established rules or standards.
Regulatory Frameworks and Guidelines – Legal and procedural structures that support the enforcement and monitoring of the Policy.
Respectful – Ensuring that users honor others' rights and exercise freedom of speech responsibly.

Safer Online Environment – A digital space that minimizes risks such as harassment, abuse, or exploitation.
Social Media – refers to online applications and platforms that enable people to create, share, and interact with content including text, images, videos and audios.
Social Media Accounts – refers to the online profiles created by individuals, organizations, or businesses on social media platforms such as Facebook, Twitter, Instagram, LinkedIn, TikTok, etc.
Social Media Platforms – Digital tool and services such as Facebook, TikTok, and others where users can interact, which are subject to compliance with laws and regulations.
Social Media Responsibility – A set of guidelines that require users to behave ethically, respect others rights, and comply with legal and moral standards when using social media platforms.
Social Media Users – refers to the individuals or entities who actively engage with social media platforms to share content, and interact with others.
Software and Application Developers – Professionals or companies creating software or digital applications.
Technology – refers to the application of scientific knowledge, tools, and techniques to create devices, systems, or processes that solve problems and improve daily activities.
Telecommunication Service Providers – Companies offering communication services, including and internet.
User Accountability – The requirement for users to adhere to policy directives, including using valid identities and avoiding harmful content.

ABBREVIATIONS

DICT - Department of Information and Communications Technology
KTDC - Kumul Technology Development Corporation
NCSC - National Cyber Security Center
NICTA - National Information and Communications Technology Authority
NIO - National Intelligence Organization
OoC - Office of Censorship
OSCA - Office of Security Coordination & Assessment
PMNEC - Department of Prime Minister and National Executive Council
RPNGC - Royal Papua New Guinea Constabulary

Table of Contents

FOREWORD BY THE MINISTER

It is an honor to present the Papua New Guinea Social Media Policy to the people of Papua New Guinea. This policy establishes a comprehensive framework to guide all social media users in the country to use social media more responsibly.

This policy is a culmination of efforts by my Department and relevant agencies. I would like to commend the Secretary and his staff including all representatives from relevant agencies involved to ensure the development of this important document. This policy document will help the development of social media regulation and complement other existing policies and legislation.

The goal of this policy is to ensure that we promote safe usage of social media platforms and to maintain our cultural and Christian values and principles as we continue to adopt and adapt to ever changing lifestyles influenced by technology advancements.

I want to inform all of us that, it is the duty of the Government to protect, promote, monitor and set guidelines to create an enabling environment for all users to be responsible while using social media for developmental purposes and from cyber-threats and to ensure national security. At this juncture, let me make a special mention to commend the Marape-Rosso Government for the bold leadership and recognition in supporting my Ministry to reform the ICT sector and transform the implementation of key ICT programs to better service Papua New Guineans.

Social media has become an integral part of our daily lives, offering a platform for communication, information sharing, and community building. It also presents its unique challenges, including the spread of misinformation and disinformation, cyberbullying, and threats to privacy and security. Hence, this policy will address these challenges while promoting freedom of expression, freedom of speech and other rights for all Papua New Guineans to be accountable.

My Department will be the lead implementing agency in collaboration with the National Information and Communications Technology Authority and National Censorship Office, including other respective state agencies, platform owners, industry players and other key stakeholders to partner and collaborate to ensure compliance. I want to encourage all Papua New Guineans to take ownership of this policy and be accountable so that we can create a safe social media environment. Let us continue to work together to embrace technological advancement to positively contribute to the development of our country.

May God continue to Bless Papua New Guinea as we celebrate the 50th Golden Jubilee of our Independence.

HON. TIMOTHY MASIU, MP
Minister for Information and Communications Technology

STATEMENT BY THE MINISTER FOR COMMUNITY DEVELOPMENT AND RELIGION

I am pleased to extend my support for the Social Media Policy. This Policy is very significant in addressing the challenges faced by the rapid expansion of social media use in our nation.

Social media has revolutionized communication, information sharing, and public engagement in Papua New Guinea, connecting individuals, businesses, and government entities.

However, this digital revolution has also introduced and posed significant challenges, including cyber harassment, misinformation, privacy breaches, and the exposure of vulnerable groups particularly children and young adults as well as digitally illiterate populations to harmful content.

It is a crucial step in ensuring that the use of digital platforms in Papua New Guinea aligns with our moral and ethical values, fosters responsible communication, and upholds social harmony. My Department will work in collaboration with the Department of Information and Communications Technology and other relevant agencies to ensure a safer and more responsible digital environment.

The Department for Community Development and Religion recognizes the importance of guiding our people, particularly our youth, in using social media responsibly. Our moral and ethical values must not be compromised in the digital space. We believe that social media should serve as a tool for constructive dialogue, national development, and the promotion of respect and dignity for all individuals.

This Policy aligns with our national commitment to promoting respect and integrity, strengthening family and community values, preventing cyber bullying and online harassment, encouraging ethical digital citizenship, and safeguarding national unity.

I urge all stakeholders, including parents, educators, businesses, and policymakers to embrace this initiative. Together, we can ensure that social media serves as a positive and productive tool for communication, education, and growth while safeguarding our citizens, particularly the most vulnerable among us.

HON. JASON PETER, MP
Minister for Community Development and Religion

SECTION ONE

1. INTRODUCTION

1. Background

Social media has become an integral part of communication, information dissemination, and public engagement. In recent times, Papua New Guinea's social media accessibility rate has increased significantly[1]. Social media has played a very important role in disseminating information. Platforms such as Facebook, Instagram, TikTok, and LinkedIn plays a significant role in connecting people with communication with individuals, business, and accessing of government services. However, the rapid evolution of social media has presented challenges including privacy breaches, misinformation, online harassment, hate speech, data security, and abuse of platforms amongst others.

Recent reports have shown high social media usage rates in Papua New Guinea. Studies indicate that approximately 10.6% of the population are active social media users as of 2024[2]. Most users are aged 18-34, with minimal representation of children under 16 years. However, young individuals who access the internet are often unsupervised, exposing them to harmful content on social media platforms. Some become victims of online harassment, leading to trauma and stress at a very young age.

To address these challenges, the Government of Papua New Guinea has taken proactive steps through policy interventions. The Minister for Information and Communications Technology has commissioned the Department of Information and Communications Technology (DICT) as the lead agency to develop a policy addressing social media issues in the country.

This initiative has prompted the Department to collaborate with the Office of Censorship, National Information and Communications Technology Authority (NICTA) and other relevant agencies, including international partners and stakeholders to outline policy directives aimed at safeguarding the use of social media platforms, with a particular focus on protecting underage children and young adults.

The Papua New Guinea Social Media Policy aims to ensure a safe, positive, and productive environment for social media use. This Policy recognizes and respects the constitutional rights to freedom of speech and freedom of press, which are fundamental democratic principles. Key objectives include reducing cyber harassment, managing misinformation, combating cyber threats, supporting economic development, assisting law enforcement and justice, and protecting vulnerable populations.

---

1 *DataReportal. (2024). Digital 2024 Papua New Guinea Overview. Retrieved from* **DataReportal**.

2 *NapoleonCat. (2023). Social Media Usage Statistics for Papua New Guinea. Retrieved from* **NapoleonCat**.

1.1. Intent of the Policy

To enable and promote responsible use of social media platforms in Papua New Guinea.

1.2. Policy Outcome

The Social Media Policy is intended for Papua New Guinea to achieve the following:

i. Ensure a safer online environment for users, particularly children under the age of 16 and young adults.

ii. Reduce incidents of cyber harassment and online abuse.

iii. Mitigate fake news, misinformation and disinformation.

iv. Strengthen socioeconomic opportunities through the safe use of digital platforms including social media.

v. Ensure regulations and compliance in addressing social media abuse, harassment and cyber threats.

vi. Foster community awareness on e-safety and encourage digital skills and development.

1.3. Target Audience

All users including children under the age of 16, platform owners and others as defined under this category.

1.4. Policy Alignment

1.4.1. National Strategic Plans

i. Papua New Guinea Vision 2050

ii. Medium Term Development Plan IV (2023 – 2027)

iii. Digital Government Plan 2023 – 2027

iv. National Cyber Security Strategy 2024 – 2030

1.4.2. Policies

i. National Information and Communications Technology Policy 2008

ii. Digital Transformation Policy 2020

iii. National Cyber Security Policy 2021

iv. National Censorship Policy II (2021-2025)

v. National Data Governance and Protection Policy 2024

1.4.3. Legislation

i. Digital Government Act 2022

ii. Cybercrime Code Act 2016

iii. Lukautim Pikinini Act (*Child Protection Act)* 2015

iv. National Information and Communications Technology Act 2009

v. Classification of Publication (*Censorship*) Act 1989

vi. National Broadcasting Cooperation Act (*Chapter 149*) 1973

SECTION TWO

2. POLICY FOCUS AREAS

The policy focuses on ensuring responsible and ethical use of social media platforms by individuals, organizations, and government entities. It aims to promote the use of social media for positive engagement, while addressing issues like misinformation, privacy concerns, and online safety.

2.1. User Accountability

This policy directs all users of social media to adhere to the following principles:

i. **Decency**: Display behavior that is acceptable and or moral whilst using social media.

ii. **Respectful**: Avoid infringing on other peoples rights whilst exercising freedom of expression and or freedom of speech in communicating and disseminating information.

iii. **Factual**: Be responsible in disseminating truthful information on social media platforms.

iv. **Legal**: Observe relevant laws and regulations guiding social media practices in the country.

v. **Privacy**: Understand and comply with community standards and privacy rights.

2.1.1. Age Restriction

This policy directs all users to comply with the following safeguard measures:

i. **Children under 16 years of age**- Parents and legal guardians must take full responsibility of children under this age group for them to access social media platforms.

ii. **Access to Social Media**- All children under the age of 16 years are prohibited from accessing sexual content and other illegal sites.

iii. **Access to Device**- Parents and legal guardians are responsible for children under the age of 16 years for accessing any digital device.

2.1.2. Social Media Accounts

i. All users of digital and social media platforms including children under the age of 16 years must have valid and legal identification to open an account.

ii. All users of digital and social media platforms including children under the age of 16 years are restricted to only three (3) personal accounts per social media platform.

iii. All users including formally registered business entities, professional bodies, institutions or organization who do business online or create blogs, pages, opinion groups or forums, or any other such accounts on social media platforms must do so with valid or legal identification.

2.2.National Security

This policy directs for the establishment of effective mechanisms to protect all citizens against cyber threats, data breaches, identity theft and any other such activities:

i. **Cyber-security**- Social media accounts and platforms will be either removed, restricted or banned if it is perceived to be of threat to national security and or likely to cause social disorder.

ii. **Data protection**- Social media accounts must not disclose and disseminate any government sensitive information on social media platforms. Any account found to disseminate any such information will be removed, restricted and banned.

iii. **Social disorder**- Social media accounts that propagate violent acts, propaganda, harassment or the spread of fake news, misinformation and or disinformation will be removed, restricted and banned.

2.3. Education and Awareness

i. This policy directs for all relevant government bodies to plan and execute digital literacy awareness programs for all social media users.

ii. This policy also directs for the integration of Cyber Ethics courses into the primary and secondary education curriculum.

2.4. Misinformation and Disinformation

This policy directs the Social Media Management Desk to monitor and manage the following:

i. **Fake news –** using social media to disseminate or spread false information.

ii. **Defamation** – using social media to tarnish other person's reputation and character.

iii. **Propaganda** – using social media to disseminate political agendas, views and narratives to promote certain ideologies, influence or destabilize social harmony.

iv. **Misleading information** – using social media to disseminate untruthful information.

v. **Rumors** – using social media to disseminate unverified information.

vi. **Hate Speech –** using social media to instigate, conspire, stir or spread certain ideologies relating to religion, sex, race or political alliance.

2.6. Platform Accountability

This policy directs for all social media platforms accessed in PNG to:

i. Legally register within the country and comply with local laws.

ii. Collaborate with the National eSafety Directorate for fact-checking to ensure enforcement in the case of national emergency, social unrest, or concerning any national security interest.

2.7. Social Media Content

This policy directs for all relevant authorities to ensure filtering of harmful content such as text, images and videos and remove, restrict or ban any user account in breach of relevant laws or regulations in Papua New Guinea.

SECTION THREE

3. ENFORCEMENT AND IMPLEMENTATION FRAMEWORK

i. The policy directs for an enforcement mechanisms to be established to enforce penalties and sanctions for non-compliance, such as fines or legal action, and includes monitoring by relevant authorities to ensure adherence.

ii. This policy directs for an establishment of an implementation framework that defines the roles and responsibilities of government agencies, stakeholders, and the public in promoting the responsible use of social media, while ensuring the policy is effectively enforced and implemented.

3.1. Establishment of National eSafety Directorate

i. This policy directs for the establishment of National eSafety Directorate to be responsible for implementation of the Papua New Guinea Social Media Policy.

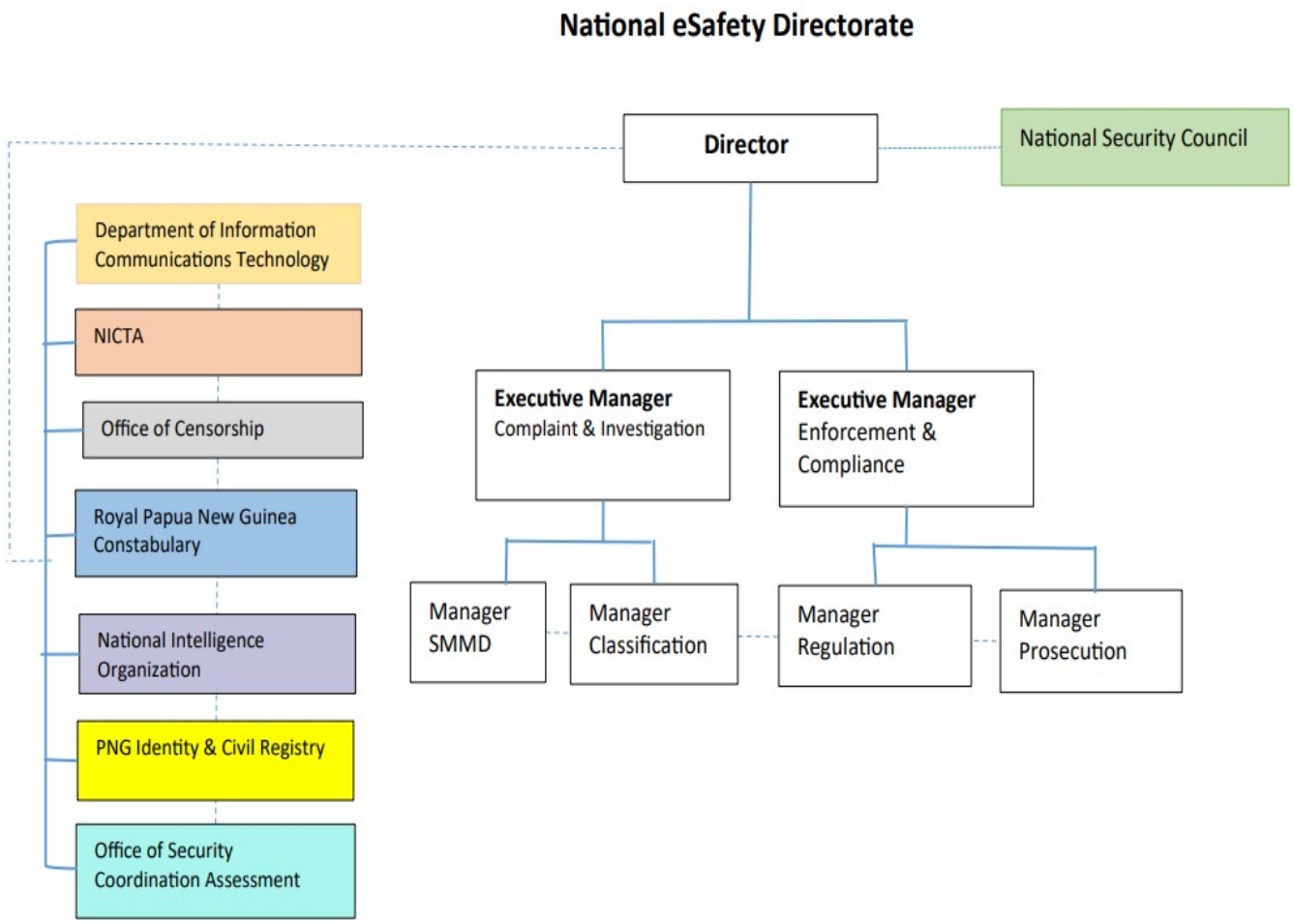
ii. The National e-Safety Directorate to be recognized and mandated to take carriage of the enforcement of this policy to ensure compliance.

iii. The National e-safety Directorate will monitor, verify and manage social media platforms including all fake news, misinformation and disinformation in the public domain that will have implications on national security and safety.

iv. This policy directs the National e-Safety Directorate to liaise and collaborate with relevant agencies in the case of national security threats or emergencies.

v. Department of Information and Communication Technology in collaboration with relevant agencies will coordinate and administer the operations of the National e-Safety Directorate.

vi. National eSafety Directorate Organizational Structure



3.2. Institutional Arrangements

i. The policy directs for a clear guidelines and roles within institutions to ensure proper management and oversight of social media usage in Papua New Guinea.

ii. These arrangements typically include designating responsible parties, setting compliance standards, and defining procedures for monitoring, enforcing, and implementing the policy.

3.2.1. Department of Information and Communications Technology

The Department of Information and Communications Technology is the lead agency and as the custodian of the Digital Government Act 2022. It is mandated to carry out functions and responsibilities related to ICT matters in the country and will provide coordination in the implementation of the policy.

i. **Coordination:** This policy directs for the Department of Information and Communications Technology in collaboration through the functions National eSafety Directorate to coordinate implementation.

ii. **Governance:** This policy directs the Department of Information and Communications Technology through the functions of the National eSafety Directorate to ensure governance.

iii. **Enforcement:** This policy directs the Department of Information and Communications Technology including other relevant agencies to collaborate with the National eSafety Directorate to ensure compliance.

3.2.2.National Information and Communications Technology Authority

The National Information and Communications Technology Authority is the regulator of the ICT sector in Papua New Guinea and it is empowered by the National Information and Communication Technology Act 2009.

3.2.3. Department of Justice and Attorney General

The Department of Justice and Attorney General is the chief legal advisory arm to the government as defined by the constitution of Papua New Guinea. It can make necessary interventions when required in terms of amendments of existing laws, drafting of new laws and regulations as well as interpretation of such laws and regulations.

3.2.4. Department for Community Development and Religion

Department for Community Development and Religion is the custodian of the Lukautim Pikinini Act 2015 (Child Protection Act). It is mandated to promote social development and safeguard vulnerable populations including children under the age of 16.

3.2.5. Royal Papua New Guinea Constabulary

Royal Papua New Guinea Constabulary is the enforcement agency as mandated by the Police Act 1998 to protect and safeguard communities in the country. It also has the mandate to enforce other subsequent legislation such as the Cyber Crime Code Act 2016.

3.2.6. Office of Censorship

The Office of Censorship is empowered by the Classification of Publication (Censorship) Act 1989. It is mandated to ensure mass media and public communications systems are free from all forms of unwanted and offensive content which is immoral and unethical.

3.2.7. National Security Council

The NSC operates under the authority of the National Security Council Act 1990. Which establishes its mandate to coordinate national security policies and strategies. It ensures a unified approach to addressing security threats, both internal and external, and advises the government on matters concerning national safety and stability.

3.2.8. Office of Security Coordination and Assessment

The OSCA functions as a subsidiary body under the NSC, with its roles and responsibilities outlined in the National Security Council Act 1990. It works closely with law enforcement agencies, intelligence bodies, and other security-related institutions to evaluate risks and enhance security measures across the country.

3.2.9. National Intelligence Organization

The NIO is governed by the National Intelligence Organization Act 1984, which portrayed its duties in intelligence gathering and analysis to protect national interests. The NIO collaborates with domestic and international agencies to prevent security breaches and ensure the protection of national interests.

3.3. Enforcement Mechanism and Implementation Framework

MECHANISM	DESCRIPTIONS	POLICY AND LEGISLATION	ENFORCEMENT AUTHORITY

Age Restriction	• Individuals aged 16 and below will be restricted from accessing certain social media platforms deemed inappropriate.	• Lukautim Pikinini Act 2015 • Classification of Publication (Censorship) Act 1989	• OoC • NICTA
Mandatory Digital ID	• Citizens aged 16 and above to use a verified SevisPass (Digital ID) to access social media platforms within the country. • All citizens to use registered sim card to have access to social media	• National Digital ID Policy 2025 • Digital Government Act 2022	• DICT • KTDC • NICTA • NID
Platform Accountability	This policy directs Social media platforms operating in PNG to: • Legally register within the country and comply with national laws. • Route their traffic through PNG's Internet Exchange Point (IXP) to ensure transparency and oversight.	• Classification of Publication (Censorship) Act 1989 • Digital Government Act 2022 • NICT Act 2009 • National Censorship Policy II 2021-2025	• OoC • DICT • NICTA
National eSafety Directorate	Provide technical support in censorship matters by monitoring and filtering misinformation, this desk ensures that false information, especially related to critical issues is identified and addressed promptly.	• Digital Government Act 2022 • Classification of Publication (Censorship) Act 1989	• DICT • OoC
Penalties	Penalties are applicable for any breach of social media laws and regulations such as cyber harassment and the spread of defamatory content online including misinformation. Imposition of penalties will be in both fines and bans or restrictions.	• Cybercrime Code Act 2016 • Digital Government Act 2022	• RPNGC • NCSC
Social Media Shutdown	In response to civil unrest, or civil disorder or for the interest of national security, the government will temporarily shut down social media platforms during states of emergency if misuse continues.	• Digital Government Act 2022 • Internal Security Act 1993	• PM & NEC • OSCA • NIO • NCSC • NICTA

3.3.1. Implementation Mechanism and Agency Coordination Flowchart

3.4. Awareness and Advocacy

This Policy directs for all relevant authorities and designated bodies to plan and execute nationwide awareness and advocacy programs, especially on digital skills and training.

SECTION FOUR

4. REGULATORY FRAMEWORKS AND GUIDELINES

4.1. Amendment of relevant legislation

This policy directs for relevant legislation(s) to be reviewed and amended to implement the Papua New Guinea Social Media Policy. It requires lawmakers to assess existing laws and make necessary modifications to support the policy's implementation.

4.2. Need for a Legislation

This policy directs the development of a Bill to provide an overarching legal framework. his law will provide clear rules and guidelines to ensure responsible use of social media. It will help protect users, prevent misuse, and support the government's efforts to manage digital communication.

4.3. Standards

This policy directs all users to observe and comply with the social media standards.

i. **Privacy Compliance**: Respect data privacy laws and global standards.

ii. **Freedom of expression**: Uphold rights to free speech while avoiding harm to others.

iii. **Transparency and integrity**: Ensure truthful and ethical conduct online.

iv. **Cyber Security Awareness**: Promote safe and secure digital practices.

v. **Terms of use adherence**: Comply with platform specific terms and conditions.

vi. **Community Standards Compliance**: Avoid prohibited activities like hate speech and harassment.

vii. **Intellectual Property Respect**: Use and share content within copyright rules.

viii. **Content Moderation Support**: Report policy violations and avoid disruptive behavior.

ix. **Responsible Engagement**: Be sensible when interacting online.

x. **Disclosure Requirement**: Clearly disclose paid partnership or promotional content.

4.4 Compliance

This policy mandates that all individuals, organizations, and entities engaging in social media activities within Papua New Guinea must adhere to the outlined social media standards. Regulatory bodies will oversee enforcement, and violations may result in penalties, restrictions, or legal action. Compliance mechanisms include:

i. **Monitoring and Reporting** – Establishing a system for tracking adherence and reporting breaches.

ii. **Enforcement Measures** – Implementing corrective actions, penalties, or suspensions for non-compliance.

iii. **Training and Awareness** – Conducting educational programs to promote understanding of social media regulations.

iv. **Audits and Assessments** – Periodic evaluations to ensure policy effectiveness and address emerging challenges.

v. **Collaboration with Platforms** – Working with social media companies to reinforce policy adherence. This framework ensures responsible social media use while protecting users and upholding national laws.

SECTION FIVE

5. MONITORING & EVALUATION

i. The policy directs the Department and Communications Technology in collaboration with the National Information Communication Technology Authority to undertake ongoing monitoring and evaluation to ensure its effectiveness and relevance.

ii. This policy directs the National eSafety Directorate to manage, assess, and provide quarterly reports on its efforts in the surveillance of social media platforms to relevant authorities and agencies for decision-making and executing their responsibilities.