ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

POLICY COMPLIANCE AND DATA SECURITY BY CYBERCAFÉS IN NAIROBI COUNTY, KENYA: AN EVALUATION OF AWARENESS OF DATA PROTECTION AND COMPUTER MISUSE AND CYBERCRIMES ACTS

Authors: Everleen Nekesa Makhanu[1], Resila A. Onyango[2] and Henry Mwenemeru[3]

[1,2&3]National Defence University-Kenya
P. O. Box 24381- 00502, Nairobi, Kenya

Abstract: *Cybercafés remain important access points for e-government and digital services in Kenya, but their shared-user environments expose personal information to unauthorized access, misuse, disclosure and residual data retention. Despite Kenya's legal framework anchored in the Data Protection Act (DPA), 2019 and the Computer Misuse and Cybercrimes Act (CMCA), 2018, empirical evidence on data-security practices among cybercafé operators remains limited. This study investigated the effect of legal awareness and cybersecurity measures on data-security outcomes among cybercafé operators in Nairobi County. An explanatory research design within a mixed-methods approach was adopted. The target population comprised an estimated 1,200 cybercafés across 17 sub-counties. Using Yamane's formula at a 5% level of precision, 300 operators were selected through stratified random sampling and proportionately allocated across the sub-counties. Eight key informants from relevant data-protection, cybersecurity, county government, law-enforcement and ICT institutions were purposively selected separately from the survey respondents. Quantitative data were collected using a structured questionnaire, while qualitative data were collected using a Key Informant Interview Guide. Quantitative data were analyzed using SPSS Version 26 through descriptive statistics, while qualitative data were analyzed thematically and reported narratively. Quantitative findings indicated high self-reported levels of legal awareness, cybersecurity measures and data-security practices. However, qualitative findings revealed that legal awareness was often superficial, cybersecurity measures were inconsistently implemented, and regulatory enforcement remained weak. The findings demonstrated a gap between awareness of data-protection requirements and their consistent application in practice. The study concluded that improving data security among cybercafés requires interventions extending beyond legal awareness to practical cybersecurity support and sustained regulatory engagement.*

Keywords: *Data security, legal awareness, cybersecurity measures, data protection, cybercafés, e-government services, regulatory compliance, cybersecurity governance, personal data protection, data security compliance*

ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

INTRODUCTION

Data security has emerged as a critical concern for governments and authorities globally as digitalization accelerates. The World Economic Forum (2024) noted a sharp rise in cyber incidents targeting small and medium-sized enterprises (SMEs) due to weak security infrastructure and fragmented regulatory compliance. Hoofnagle *et al*. (2019) and Bridson (2025) in separate publications, acknowledge that international frameworks such as the European Union's General Data Protection Regulation (GDPR), the Council of Europe Convention 108+ (1981), the OECD Privacy Guidelines (2026) and the APEC Privacy Framework (2004) have established stringent standards for lawful data processing and privacy protection, highlighting vulnerabilities in shared ICT environments. In Africa, the Malabo Convention seeks to harmonize data governance, though, according to a 2020 report by the African Union (AU), the ratification and enforcement remain uneven. Closer home, Daniel (2025) analyzed East African Community frameworks as similarly advocating coordinated data-protection standards, yet findings revealed that implementation gaps persist due to limited institutional capacity and widespread ICT informality.

In Kenya, the Data Protection Act (DPA), 2019, enacted to give effect to Article 31(c) and (d) of the Constitution of Kenya (2010), provides the principal legal framework for the protection and lawful processing of personal data. The Act establishes a comprehensive set of data-protection principles requiring data controllers and processors, including cybercafés that process personal information on behalf of clients, to ensure that personal data are processed lawfully, fairly and transparently; collected for explicit, specified and legitimate purposes; limited to what is necessary; maintained accurately; retained only for as long as necessary; and protected through appropriate measures that ensure integrity, confidentiality and accountability. These principles are particularly relevant to cybercafés because their routine services often involve collecting, accessing, transmitting, storing and temporarily retaining customers' sensitive personal information. Data Protection Laws Kenya (2024) noted that Sections 25 and 26 of the DPA, 2019 place specific obligations on data processors to ensure lawful processing, purpose limitation, integrity and confidentiality, thereby requiring cybercafés to adopt appropriate safeguards throughout the data-processing cycle. The Act further provides for accountability in data processing, making operators responsible for demonstrating compliance with established data-protection requirements. Complementing the DPA, the Computer Misuse and Cybercrimes Act (CMCA), 2018 provides a broader cybersecurity framework by criminalizing offences such as unauthorized access to computer systems, illegal access to or interference with data, and other forms of computer-related abuse, while providing for collaboration among relevant institutions, including the Office of the Data Protection Commissioner (ODPC) and the Communications Authority of Kenya (CA). Collectively, these legal instruments provide a strong regulatory foundation for safeguarding personal information; however, their effectiveness among cybercafé operators depends largely on the operators' awareness of their legal obligations, adoption of appropriate cybersecurity measures, and the capacity of regulatory institutions to monitor and enforce compliance.

ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

The vulnerability of cybercafés is heightened by their predominantly small-scale and informal operating environment. Unlike large corporations and government institutions, many cybercafés have limited financial resources, inadequate technical expertise, weak internal controls and limited access to specialized cybersecurity personnel. This concern is particularly significant because cybercafés routinely process sensitive personal data, including scanned national identification documents, biometric credentials and government portal login information. Munyendo et al. (2023) found that many cybercafé operators had limited understanding of their data-protection obligations, while Juma and Faturoti (2025) reported that enforcement of data-protection requirements at informal digital-access points remained weak. With Kenya's e-government ecosystem expanding from approximately 5,000 services in 2023 to over 22,500 by 2025, as reported by the Huduma Kenya Secretariat, citizens' reliance on cybercafés as digital intermediaries has increased, potentially amplifying risks of unauthorized disclosure, residual data retention and identity theft. Although legal awareness may enable operators to better understand and comply with data-protection requirements, awareness alone may not guarantee secure data processing in the absence of practical cybersecurity measures, including access controls, secure networks, password protection, updated software, antivirus protection, secure storage and proper deletion of customer information. Moreover, the broader political and regulatory environment may influence the extent to which legal awareness and cybersecurity measures translate into improved data-security outcomes. Despite these concerns, existing scholarship, including Masinde et al. (2025) and Mburu (2024), has largely focused on formal institutions such as banks, government agencies and corporations, with limited empirical attention to informal digital-access points. This gap necessitates empirical investigation of the effect of legal awareness and cybersecurity measures on data-security outcomes among cybercafé operators in Nairobi County, Kenya.

METHODOLOGY

An explanatory research design within a mixed-methods approach was adopted to determine why and how legal awareness, cybersecurity measures and political environment influence data security outcomes among cybercafé operators in Nairobi County (Creswell & Creswell, 2018). Triangulating quantitative and qualitative data enabled cross-verification of results and reduced bias.

The target population comprised an estimated 1,200 cybercafés, both licensed (221 with active Unified Business Permits per County Government of Nairobi, 2026) and unlicensed operators identified through field reconnaissance, across Nairobi County's 17 sub-counties. The estimate was derived from the Kenya National Bureau of Statistics (2022) report on small ICT-based enterprises operating in Nairobi County, which documented a significant number of informal and semi-formal cybercafé operations beyond those formally licensed.

Using Yamane's (1967) formula [$n = N / (1 + Ne^2)$], with N = 1,200 and e = 0.05, a sample of 300 was derived. An additional 10% buffer gave an adjusted sample of 330. Within each of the 17 geostrata: Dagoretti North, Dagoretti South, Embakasi Central, Embakasi East, Embakasi North,

ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

Embakasi South, Embakasi West, Kamukunji, Kasarani, Kibra, Lang'ata, Makadara, Mathare, Roysambu, Ruaraka, Starehe and Westlands, cybercafés were allocated proportionally using the formula nh = Nh × n / N (Table 1). For the qualitative component, 8 key informants were selected purposively, separately from the 300 survey respondents, as detailed in Table 2.

Table 1: Stratified Sampling Matrix, Nairobi's 17 Sub-Counties

Sub-County	Target Population	Sample Allocated
Dagoretti North	104	26
Dagoretti South	108	27
Embakasi Central	32	8
Embakasi East	68	17
Embakasi North	56	14
Embakasi South	72	18
Embakasi West	64	16
Kamukunji	116	29
Kasarani	92	23
Kibra	60	15
Lang'ata	56	14
Makadara	60	15
Mathare	44	11
Roysambu	32	8
Ruaraka	48	12
Starehe	84	21
Westlands	104	26
Total	**1,200**	**300**

Source: Researcher (2026); County Government of Nairobi (2026)

Table 2: Key Informant Interview (KII) Sample

Category of Key Informant	No.	Tool
ODPC	2	KII Guide
CA	2	KII Guide
County Government of Nairobi – Licensing Department	1	KII Guide
National Police – Cybercrime Unit Officer	1	KII Guide
NC4 Representative	1	KII Guide
ISP Representative	1	KII Guide
Total	**8**	

Source: Researcher (2026)

Primary data was collected using a structured questionnaire (quantitative) and a Key Informant Interview (KII) Guide (qualitative), after obtaining ethical approvals from the National Defence University – Kenya and NACOSTI. Quantitative data was analyzed using SPSS Version 26, generating descriptive statistics, correlation analysis, binary logistic regression and hierarchical

ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

moderation regression. Qualitative data was analyzed thematically following Braun and Clarke's (2006) six-phase framework. Findings were integrated through triangulation.

RESULTS

Demographic Profile

Of the 330 questionnaires distributed, 300 were returned (90.9% response rate). Respondents were predominantly male (75.3%), with 24.0% female and 0.7% undisclosed. The majority (66.0%) were aged below 25 years, followed by 25–34 years (32.3%). Regarding education, 48.0% held secondary-level qualifications, 38.7% had diplomas, 12.0% had degrees and 1.3% had primary education only, consistent with the predominantly young, informally trained cybercafé workforce in Nairobi County.

Legal Awareness

Table 3 presents descriptive statistics for the five legal awareness items.

Table 3: Legal Awareness Descriptive Statistics

Statement	SD	D	N	A	SA	Mean	SD
Familiar with DPA provisions relevant to cybercafés	0.0%	0.0%	2.7%	82.3%	15.0%	4.12	0.40
Understand legal responsibilities regarding customer data protection	0.3%	2.7%	3.3%	84.0%	9.7%	4.00	0.52
Aware of penalties and sanctions for non-compliance	0.0%	1.0%	4.3%	81.0%	13.7%	4.07	0.46
Received training/guidance on legal requirements for data security	0.0%	13.7%	28.3%	47.3%	10.7%	3.55	0.86
Understand customers' rights on collection and use of personal data	0.0%	1.0%	2.7%	83.3%	13.0%	4.08	0.44
Average						**3.96**	**0.23**

Source: Researcher (2026). SD = Strongly Disagree; D = Disagree; N = Neutral; A = Agree; SA = Strongly Agree.

A large majority (97.3%) reported familiarity with DPA 2019 provisions applicable to cybercafés (mean = 4.12, SD = 0.40); 93.7% understood their legal responsibilities (mean = 4.00, SD = 0.52); and 94.7% were aware of penalties for non-compliance (mean = 4.07, SD = 0.46). Understanding of customer data rights was high at 96.3% (mean = 4.08, SD = 0.44). However, only 58.0% had received formal training or guidance on legal requirements for data security (mean = 3.55, SD =

ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

0.86), the lowest mean and highest standard deviation across all items, indicating that structured legal education for cybercafé operators remains limited. The overall mean was 3.96, reflecting moderately high self-reported awareness. Qualitative findings corroborated superficial knowledge:

> Only about 25% of cafés we visit actually know what the seven principles mean. Most think registration with us is the end of it (ODPC Officer, KII001)

> Cybercafé operators, when asked about purpose limitation or data minimization, just give blank faces (CA Officer, KII005)

Cybersecurity Measures

The overall average mean for cybersecurity measures was 4.04 (SD = 0.56), indicating generally high self-reported implementation. System monitoring recorded the highest mean (4.17, SD = 0.46), while antivirus and firewall protection recorded the lowest (mean = 3.74, SD = 0.75), with 10.0% of respondents disagreeing that their cybercafés had up-to-date antivirus and firewall protection. Qualitative evidence revealed that available technical tools are implemented reactively and inconsistently, with shared computers lacking automatic session log-outs and forced data deletion.

Political Environment

The political environment received the lowest ratings of all variables (overall mean = 2.77, SD = 0.78). A total of 81.3% disagreed that there is strong political support for data protection enforcement (mean = 2.26, SD = 0.79), and 77.3% disagreed that government leadership prioritizes data security (mean = 2.35, SD = 0.84). In contrast, 95.7% agreed that political interference affects enforcement activities (mean = 3.97, SD = 0.42). Qualitative findings portrayed governance as distant and enforcement as reactive rather than systematic.

DISCUSSION

The study found that legal awareness is a positive and significant predictor of data security outcomes ($r = 0.615$, $p = 0.000$; $\beta = 0.465$, $p = 0.000$). The gap between what operators say they know and what they do is consistent with Compliance Theory, which Tyler (2006) holds that low normative knowledge of legal obligations essentially undermines voluntary compliance with regulations. The study revealed notable interest in government-sponsored training, showing a clear need for structured compliance training, and confirms that although the baseline legal awareness of cybercafé operators is present, this awareness is not consistently reflected in the practice of data protection. These findings are consistent with Masinde *et al*. (2025), who found that data privacy awareness in Kenya remained critically low despite an existing regulatory landscape, and with Odhiambo and Wekesa (2024), who reported that no meaningful improvement in legal literacy among cybercafé operators had occurred since the enactment of the DPA in 2019. Munyendo *et al*. (2023) similarly documented that 80% of Nairobi cybercafé operators lacked practical data-

ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

handling knowledge despite daily engagement with sensitive e-government documents. This study contributes new empirical evidence by establishing legal awareness as the strongest single predictor of data security in Kenya's post-DPA 2019 informal cybercafé sector.

Cybersecurity measures were confirmed as a positive and significant predictor of data security ($r = 0.583$, $p = 0.000$; $\beta = 0.414$, $p = 0.000$). The comparable standardized beta coefficients indicate that technical controls and legal knowledge work together rather than independently. Qualitative evidence of reactive and inconsistent implementation, antivirus tools constrained by cost, power outages and outdated hardware, confirms research findings by Von Solms & Van Niekerk in 2013 that isolated technical tools cannot achieve the CIA triad without systematic organizational embedding. Additionally, these findings mirror Munyendo *et al*. (2023) and King'ori (2014), who documented weak session management and residual data exposure despite occasional antivirus use, and extend those findings into the post-DPA 2019 era.

The political environment was confirmed as a significant moderator, with R-square increasing from 0.569 to 0.651 upon introducing interaction terms, demonstrating that political context amplifies the positive effects of both legal awareness and cybersecurity measures on data security outcomes. Operators' negative perceptions of political commitment and qualitative portrayals of "distant governance" and "reactive enforcement" confirm that macro-level political will has not translated into micro-level support, consistent with Juma and Faturoti (2025) and Daniel (2025). From the Compliance Theory perspective (Tyler, 2006), visible deterrence and regulatory legitimacy are critical preconditions for compliance behaviour, and their absence structurally limits the translation of legal knowledge and technical tools into secure data practices on the ground.

CONCLUSION

Despite Kenya's progressive and internationally aligned data protection and cybersecurity legal framework, there exists a profound and systemic implementation gap at the level of Nairobi County cybercafés, critical intermediaries for millions of citizens accessing e-government services. Legal awareness and cybersecurity measures are empirically significant positive predictors of data security, and the political environment significantly moderates these relationships; yet structural realities of pervasive informality, resource constraints, high staff turnover, outdated hardware and chronically weak enforcement capacity limit the translation of legal knowledge and technical tools into secure data practices. Improving data security in cybercafés requires more than legal knowledge and basic technical safeguards; it demands visible enforcement, affordable compliance support and stronger institutional coordination.

ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

Based on the findings, the study recommended that the Office of the Data Protection Commissioner (ODPC), in collaboration with the Communications Authority of Kenya (CA) and county governments, should introduce mandatory, low-cost, sector-specific legal awareness clinics linked to the annual Unified Business Permit renewal cycle. These clinics should provide simplified compliance guides on the seven principles of the Data Protection Act (DPA), 2019, using language and practical examples appropriate for cybercafé operators with secondary and diploma-level education. The study further recommended that the CA, in partnership with major Internet Service Providers (ISPs), including Safaricom, Zuku, Airtel and Telkom, and relevant national cybersecurity agencies, should develop subsidized "Secure Cybercafé Kits" comprising licensed antivirus software, configurable automatic session-logout tools and a concise data-handling checklist to facilitate affordable adoption of basic cybersecurity safeguards. In addition, the CA should establish Digital Compliance Desks across Nairobi County's 17 sub-counties to provide centralized points of contact for cybercafé operators seeking registration assistance, compliance guidance, cybersecurity support and access to subsidized security tools. Collectively, these interventions would shift the regulatory approach from predominantly reactive enforcement towards continuous, preventive and supportive compliance, thereby strengthening legal awareness, improving cybersecurity practices and enhancing data-security outcomes among cybercafé operators.

REFERENCES

African Union. (2020). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

African Union Commission & OECD. (2024). Africa's Development Dynamics 2024: Skills, Jobs and Productivity. https://doi.org/10.1787/df06c7a4-en

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bridson, B. (2025, August 18). The Impact of Data Privacy Regulations on Global Business & Governance. Uncover IE. https://www.ie.edu/uncover-ie/the-impact-of-data-privacy-regulations-on-global-business-governance/

Council of Europe Convention 108. (1981). Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

County Government of Nairobi. (2026). Business Permits, Cybercafés with Active Unified Business Permits Q1 2026. Nairobi City County Directorate of Trade Licensing.

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). Sage.

ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

Daniel, E. M. (2025). Harmonizing Data Protection in East Africa: A Comparative Analysis and Policy Recommendations. African Journal of Information and Communication, 13(6).

Data Protection Laws Kenya. (2024). Data Protection Laws Kenya. Office of the Data Protection Commissioner. https://www.odpc.go.ke/data-protection-laws-kenya/

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-organisational Perspectives. Information Systems Journal, 11(2), 127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and What it means. Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Huduma Kenya Secretariat. (2023). Huduma Kenya Digitalization Plan 2023/2024–2025/2026. HKS. https://www.hudumakenya.go.ke/HUDUMAKENYADIGITALIZATIONPLAN-V1.5.1.pdf

Juma, I., & Faturoti, B. (2025). Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice. International Review of Law, Computers & Technology. https://doi.org/10.1080/13600869.2025.2506918

King'ori, S. M. (2014). An Assessment of cybercafé security practices in Nairobi County, Kenya [Unpublished thesis]. University of Nairobi.

Masinde, J., Mugambi, F., & Muthee, D. W. (2025). Big data and personal information privacy in developing countries: Insights from Kenya. Frontiers in Big Data, 8, 1532362. https://doi.org/10.3389/fdata.2025.1532362

Mburu, R. (2024). An evaluation on the effectiveness of the laws on protection of personal data in Kenya [Unpublished paper]. University of Nairobi.

Munyendo, C. W., Acar, Y., & Aviv, A. J. (2023). "In Eighty Percent of the Cases, I Select the Password for Them": Security and privacy challenges at cybercafés in Kenya. In 2023 IEEE Symposium on Security and Privacy (pp. 570–587). IEEE. https://doi.org/10.1109/SP46215.2023.10179288

ODPC. (2024). What we do. Office of the Data Protection Commissioner. https://www.odpc.go.ke/functions-of-the-office/

Odhiambo, J., & Wekesa, M. (2024). Data handling practices and compliance among Nairobi-based ICT micro-enterprises. Journal of African Digital Policy, 3(1), 58–76.

Republic of Kenya. (2018). Computer Misuse and Cybercrimes Act, No. 5 of 2018. Government Printer.

ISSN: 2312-0134
African Research Journal of Education and Social Sciences, 13 (2), 2026 | Website: www.arjess.org

http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

Republic of Kenya. (2019). Data Protection Act, No. 24 of 2019. Government Printer. https://www.odpc.go.ke/wp-content/uploads/2024/02/TheDataProtectionAct__No24of2019.pdf

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database, 38(1), 60–80. https://doi.org/10.1145/1216218.1216224

Tyler, T. R. (2006). Why people obey the law. Princeton University Press.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. WEF Publications. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Yamane, T. (1967). Statistics: An Introductory Analysis. Harper & Row.