

Users' Awareness of Sharing Sensitive Information with AI Tools: A Study among University Students in Mogadishu, Somalia

Abdirahman Abdullahi Mohamud and Abdullahi Mohamud Sharif
Baacil Institute for Research and Development, Mogadishu, Somalia
<https://baacil.com>

DOI: <https://doi.org/10.70806/f3zyeg18>

Abstract

The rapid diffusion of generative artificial intelligence (AI) tools such as ChatGPT has transformed how university students access information, yet it has simultaneously raised pressing concerns about the disclosure of sensitive personal data to conversational AI systems. This study examines the awareness, behaviours, and risk perceptions of university students in Mogadishu, Somalia, regarding the sharing of sensitive information with AI tools. A cross-sectional descriptive survey was conducted between January and April 2026 with 309 respondents recruited through a systematic sampling approach, and data were analysed using Python (pandas, scipy) with descriptive statistics and Pearson's chi-square (χ^2) tests of independence. The findings show that ChatGPT was overwhelmingly the most-used tool (89.0%, $n = 275$), and 50.8% ($n = 157$) of respondents used AI tools daily. While most information shared was educational (54.4%, $n = 168$) or general queries (54.4%, $n = 168$), a notable minority disclosed work-related (13.9%, $n = 43$) and outright sensitive financial or health data (4.9%, $n = 15$). Awareness was mixed:

respondents were almost evenly split on whether they read AI privacy policies (49.5% Yes), and 29.1% admitted to having shared personal information with an AI. A majority reported low confidence in AI privacy (51.1%, $n = 158$) and doubted that the government holds sufficient power to protect them (47.2%, $n = 146$), with mean trust in AI companies of only 5.55 out of 10. Chi-square analysis revealed that reading privacy policies ($\chi^2 = 22.68$, $p < 0.001$) and privacy confidence ($\chi^2 = 32.37$, $p < 0.001$) varied significantly by education level, as did the disclosure of personal information ($\chi^2 = 12.28$, $p = 0.031$). The study evidences a clear privacy paradox: high adoption coupled with limited protective behaviour and low institutional trust. It recommends targeted digital-literacy and data-protection education, and the operationalisation of Somalia's Data Protection Act (Law No. 005 of 2023) and the Data Protection Authority to safeguard citizens in the AI era.

Keywords: artificial intelligence; ChatGPT; data privacy; privacy paradox; data protection; Somalia

Introduction

Generative artificial intelligence (AI) tools, led by OpenAI's ChatGPT and followed by Google Gemini, DeepSeek and Microsoft Copilot, have moved from novelty to everyday infrastructure within a few years. For university students, these conversational systems now serve as study companions, writing aids, coding assistants and informal advisers. The convenience of typing a question into a chatbot and receiving an instant, human-like answer has driven adoption to near-saturation among young, connected populations. Yet this same conversational intimacy invites users to disclose information they might never type into a public search engine, including personal opinions, work documents, and even financial or health details.

The privacy risks of this behaviour are substantial and increasingly well documented. Large language models are trained on vast corpora and may memorise or inadvertently reproduce sensitive data; free-tier services frequently use user prompts to further train their models; and analyses of publicly shared chatbot conversations have revealed users inadvertently exposing personally identifiable information, confidential material and intimate emotional disclosures. Because users often feel anonymous within a chat interface, they may share personal data without recognising that it can be stored, analysed, monetised, or leaked.

These concerns are amplified in developing-country contexts, where data-protection

regulation is nascent and digital-literacy interventions are scarce. Somalia enacted its Data Protection Act (Law No. 005 of 2023) and established a Data Protection Authority (Hay'adda Dhowrista Xogta Soomaaliyeed) to regulate the processing of personal data (Federal Republic of Somalia, 2023); implementing regulations under the Act were approved by the Council of Ministers in January 2026 (Somalia Data Protection Authority, 2026), but the practical reach of these instruments over global AI platforms remains untested. Within the East African Community (EAC) and the wider Horn of Africa, harmonised data-governance frameworks are still emerging, leaving individual users as the first and often only line of defence for their own data.

Mogadishu, as Somalia's largest urban and academic hub, hosts a young, mobile-first student population that has embraced AI tools enthusiastically. Understanding how these students perceive and manage the privacy risks of disclosing sensitive information to AI is therefore both timely and necessary. The literature on AI privacy awareness is dominated by studies from high-income settings; empirical evidence from Somalia and comparable contexts is almost entirely absent.

The phenomenon of interest is best framed through the 'privacy paradox' — the well-established discrepancy between users' stated privacy concerns and their actual disclosure behaviour. If Somali students, like users

elsewhere, express concern yet continue to share freely, the policy response must move beyond awareness-raising alone toward structural protections and trustworthy institutions.

This study therefore aims to:

- (i) profile the AI tools used by university students in Mogadishu and the frequency of their use;
- (ii) characterise the types of information — including sensitive personal data — that students share with AI tools;
- (iii) assess students' awareness of AI privacy policies and data-protection risks;
- (iv) measure students' trust in AI companies and confidence in the privacy of their interactions;
- (v) examine protective behaviours and attitudes, including verification of AI content and willingness to share confidential material; and
- (vi) test whether awareness and risky-sharing behaviours vary significantly by sex, education level, and field of study.

Literature Review

This review draws on a systematic search of recent peer-reviewed literature (2021–2026) addressing privacy in generative AI, self-disclosure behaviour, and data-protection awareness, with particular attention to developing-country and African evidence. Four thematic strands emerge.

Privacy and Data-Protection Risks of Generative AI

A growing body of work documents the structural privacy risks of large language models (LLMs). Survey research on privacy issues in LLMs catalogues memorisation, training-data leakage, and membership- and attribute-inference attacks as core threats (Neel & Chang, 2023; Yan et al., 2024). Studies focused specifically on ChatGPT argue that the platform treats privacy narrowly as the direct disclosure of user data rather than adopting a broader contextual definition, leaving wide gaps in user protection (Ullah et al., 2024). Industry analyses report that a meaningful share of employee prompts to AI tools contain sensitive data, and that over half of sensitive-data leaks occur on free-tier platforms that train on user queries (Kiteworks, 2024). These risks are compounded by regulatory uncertainty: the European Data Protection Board's December 2024 opinion clarified that AI models trained on personal data are not automatically anonymous and remain subject to data-protection law (Cloud Security Alliance, 2025).

User Awareness and Disclosure of Sensitive Information to AI Tools

Empirical studies increasingly probe what users actually disclose and how aware they are of the risks. Dahabiyeh et al. (2026) examined privacy awareness among ChatGPT users and found that awareness of specific privacy-policy dimensions shaped continued-use intentions. Work on privacy reasoning during chatbot use shows that, while frequent users report greater awareness of

data-collection practices, this awareness does not necessarily translate into greater trust or more protective behaviour (Nezhad et al., 2026). Contextual-integrity analyses report that respondents perceive chatbot data as highly sensitive — more sensitive than email or social-media content — yet continue to disclose because the conversational interface fosters a feeling of anonymity (Tran et al., 2025). Studies of sensitive health conversations with ChatGPT identify perceived anonymity, convenience, and non-judgement as key drivers of self-disclosure (Kelly et al., 2025).

The Privacy Paradox and Online Self-Disclosure

The privacy paradox — the gap between privacy attitudes and disclosure behaviour — is one of the most replicated findings in privacy research (Taddicken, 2014). Explanations range from privacy cynicism and low response-efficacy to temporally discounted cost-benefit trade-offs in which immediate rewards outweigh distant privacy costs (Hallam & Zanella, 2017). Experimental work demonstrates that privacy awareness and trust jointly shape willingness to self-disclose personal and health data online, with trust often overriding stated concern (Herbert et al., 2021). The paradox provides the central interpretive lens for the present study.

Data-Protection Awareness in Students and Developing Countries

Evidence from Africa and other developing regions indicates persistent gaps in privacy and information-security awareness. A diagnostic

survey of 287 students in a developing-country higher-education sector found high awareness and strong expectations but markedly lower confidence in institutional compliance, with the largest deficits in privacy education and consent (Maguraushe et al., 2026). Studies in Kenya report that the majority of incoming university students lack adequate information-security awareness (Ndiege & Okello, 2018) and that data-protection laws are difficult to operationalise against large data processors (Masinde et al., 2025). Research on data privacy across the African continent highlights the tension between rapid digitalisation and immature regulatory enforcement (Prinsloo & Kaliisa, 2022). For Somalia specifically, scholarship on ICT and digital readiness is emerging but remains sparse (Issa-Salwe et al., 2024), and within the HAJ corpus, prior work has documented digital-skills deficits in Somali institutions (Hussein & Sharif, 2025) and the early, uneven adoption of AI in Mogadishu university curricula (Hirsi & Sharif, 2026).

Research Gap

Across these four strands, a clear gap emerges. The privacy-paradox and AI-disclosure literature is overwhelmingly grounded in high-income settings; developing-country evidence is concentrated in cybersecurity and social-media contexts rather than generative AI; and no published empirical study, to the authors' knowledge, examines the awareness and disclosure of sensitive information to AI tools

among Somali university students. This study addresses that gap by providing the first quantitative profile of AI-privacy awareness, disclosure behaviour and institutional trust among university students in Mogadishu, framed against Somalia's new data-protection architecture.

Methodology

Research Design

A cross-sectional descriptive survey design was employed. This design is appropriate for collecting data at a single point in time and for systematically describing patterns in the attitudes, behaviours, and perceptions of a defined population (Creswell, 2014).

Setting and Study Period

The study was conducted among university students and recent graduates in Mogadishu, Somalia, the country's principal academic and commercial centre. Data were collected online between January and April 2026.

Study Population and Sampling

A total of 309 participants were recruited using a systematic sampling approach, based on availability and willingness to participate. Respondents were drawn from a range of fields of study and education levels to capture variation across the student population.

Data Collection Instrument

Data were collected using a structured, self-administered questionnaire comprising 23 items distributed electronically via Google Forms. The

instrument was reviewed for clarity and cultural appropriateness, and items were presented bilingually in English and Somali. The questionnaire covered five domains: (i) sociodemographic characteristics; (ii) AI-tool usage and frequency; (iii) types of information shared and disclosure of personal data; (iv) awareness of privacy policies, targeted advertising, and trust in AI companies and government; and (v) attitudinal items on privacy risk perception and protective behaviour measured on a five-point Likert scale.

Data Analysis

Data were analysed using Python (pandas, scipy). Descriptive statistics — frequencies and percentages — were computed for all variables. Multi-select items were disaggregated using binary indicator coding. Bivariate associations between categorical variables were assessed using Pearson's chi-square (χ^2) test of independence, with $p < 0.05$ as the threshold for significance. Cross-tabulations were produced for awareness and disclosure outcomes by sex, by education level, and by field of study (24 free-text fields grouped into six categories). For the chi-square tests, privacy confidence was dichotomised into 'Confident/Very confident' versus 'Not confident'. Where expected cell counts fell below five, results were interpreted with appropriate caution.

Ethical Considerations

The study was conducted under the Baacil Institute research programme [OWNER: confirm

whether reviewed/approved by the Somalia Researchers Association (SRA), as stated in the published sister article]. All participation was voluntary. Informed consent was obtained prior to data collection, and respondents were assured of the confidentiality and anonymity of their responses. Data were used solely for research purposes.

Results

Sociodemographic Characteristics

Table 1 presents the sociodemographic characteristics of the 309 respondents. The sample was predominantly young, with most aged 18–24 (59.5%, $n = 184$), and male (74.4%, $n = 230$). The majority were single (75.4%, $n = 233$) and currently students by occupation (63.1%, $n = 195$). In terms of education, Bachelor-degree holders formed the largest group (43.7%, $n = 135$), followed by diploma (21.0%, $n = 65$) and secondary-school (19.1%, $n = 59$) respondents, while postgraduate respondents (Master and PhD) together comprised 8.4% ($n = 26$). Computer Science / IT was the most represented field of study (27.5%, $n = 85$), reflecting the technology-oriented profile of the sample.

Table 1. Sociodemographic Characteristics of Respondents (N = 309)

Characteristic	n (%)
<i>Age</i>	
Under 18	46 (14.9%)
18-24	184 (59.5%)
25-34	56 (18.1%)
35-49	16 (5.2%)
50+	7 (2.3%)
<i>Sex</i>	
Male	230 (74.4%)
Female	79 (25.6%)
<i>Marital status</i>	
Single	233 (75.4%)
Married	66 (21.4%)
Divorced	10 (3.2%)
<i>Education level</i>	
Primary School	24 (7.8%)
Secondary School	59 (19.1%)
Diploma	65 (21.0%)
Bachelor Degree	135 (43.7%)
Master Degree	19 (6.1%)
PhD	7 (2.3%)
<i>Field of study (grouped)</i>	
Computer Science / IT	85 (27.5%)
Health Sciences	64 (20.7%)
Education	56 (18.1%)
Business / Economics	44 (14.2%)
Social Sciences	37 (12.0%)
Other	23 (7.4%)
<i>Occupation status</i>	
Student	195 (63.1%)
Employed	79 (25.6%)
Self-employed	21 (6.8%)
Unemployed	14 (4.5%)

AI-Tool Usage and Frequency

Table 2 presents the AI tools used by respondents. ChatGPT was by far the dominant tool (89.0%, $n = 275$), followed by Gemini (35.9%, $n = 111$), DeepSeek (15.2%, $n = 47$) and Copilot (9.1%, $n = 28$); because respondents could select multiple tools, percentages sum to more than 100%. Usage was intensive: 50.8% ($n = 157$) reported using AI tools daily and a further 19.4% ($n = 60$) weekly, while only 4.9% ($n = 15$) reported never using them. This near-ubiquitous, high-frequency adoption establishes

the exposure context within which privacy risks accumulate (Dahabiyeh et al., 2026).

Table 2. AI Tools Used by Respondents (Multi-select)

Characteristic	n (%)
ChatGPT	275 (89.0%)
Gemini	111 (35.9%)
DeepSeek	47 (15.2%)
Copilot	28 (9.1%)

Table 3. Frequency of AI-Tool Use

Characteristic	n (%)
Daily	157 (50.8%)
Weekly	60 (19.4%)
Monthly	30 (9.7%)
Rarely	47 (15.2%)
Never	15 (4.9%)

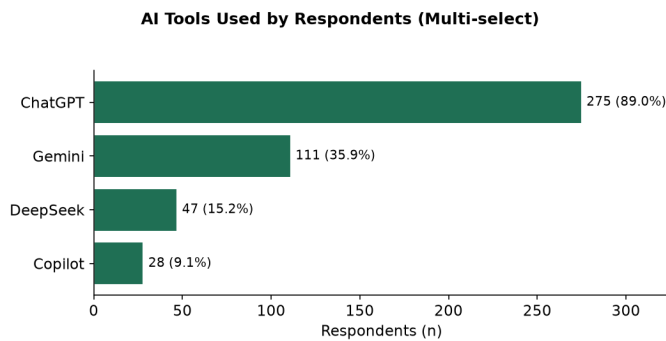


Figure 1. AI tools used by university students in Mogadishu (multi-select).

Types of Information Shared with AI Tools

Table 4 presents the types of information respondents share with AI tools. Educational content (54.4%, n = 168) and general questions only (54.4%, n = 168) were the most common, indicating that most use is task-oriented. However, a meaningful minority shared work-related information (13.9%, n = 43) and personal opinions (11.7%, n = 36), and 4.9% (n = 15) reported sharing outright sensitive data such as financial, health, or password information. This

minority is precisely the population most exposed to disclosure harm (Kiteworks, 2024).

Table 4. Types of Information Shared with AI Tools (Multi-select)

Characteristic	n (%)
Education	168 (54.4%)
General Questions Only	168 (54.4%)
Work Related Information	43 (13.9%)
Personal Opinion	36 (11.7%)
Sensitive data (financial, health, password)	15 (4.9%)

Types of Information Shared with AI Tools (Multi-select)

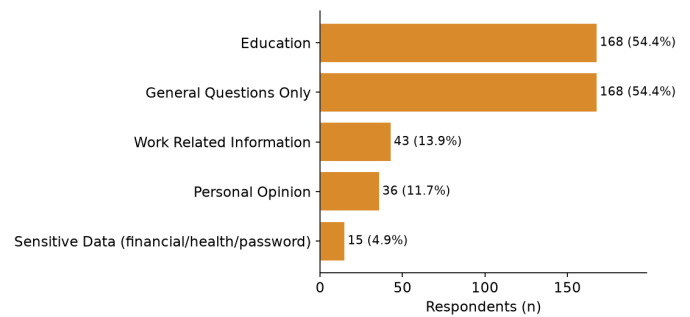


Figure 2. Types of information shared with AI tools (multi-select).

Awareness of Privacy Policies and Disclosure of Personal Information

Table 5 presents respondents' privacy-policy awareness and disclosure behaviour. Respondents were almost evenly divided on whether they read the privacy policy of AI tools before using them, with 50.5% (n = 156) reporting that they do not. Notably, 29.1% (n = 90) admitted to having shared their personal information with an AI at some point. With respect to data exploitation, 41.4% (n = 128) reported sometimes noticing advertisements on social media that appeared directly related to a private query made to an AI chatbot, and a further 15.2% (n = 47) noticed this all the time,

leaving only 43.4% (n = 134) who never noticed such targeting.

Table 5. Privacy-Policy Awareness and Disclosure Behaviour

Characteristic	n (%)
<i>Reads AI privacy policy before use</i>	
Yes	153 (49.5%)
No	156 (50.5%)
<i>Ever shared personal information with AI</i>	
Yes	90 (29.1%)
No	219 (70.9%)
<i>Noticed targeted ad linked to AI query</i>	
Never	134 (43.4%)
Sometimes	128 (41.4%)
All the time	47 (15.2%)

power to protect them from AI-related privacy breaches, and a further 37.2% (n = 115) were unsure.

Table 6. Privacy Confidence and Trust in Institutions

Characteristic	n (%)
<i>Confidence in privacy when using AI</i>	
Very Confident	48 (15.5%)
Confident	103 (33.3%)
Not Confident	158 (51.1%)
<i>Government has enough power to protect</i>	
Yes	48 (15.5%)
Not sure	115 (37.2%)
No	146 (47.2%)
<i>Trust in AI companies (1–10 scale)</i>	
Low trust (1–4)	85 (27.5%)
Moderate trust (5–7)	159 (51.5%)
High trust (8–10)	65 (21.0%)

Privacy Awareness and Risk Perception Indicators

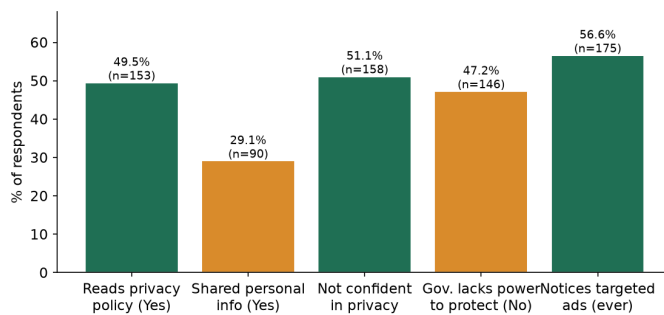


Figure 3. Privacy awareness and risk-perception indicators.

Confidence, Trust, and Perceived Government Capacity

Table 6 presents respondents' confidence and trust. A majority reported being not confident about privacy when using AI (51.1%, n = 158), while only 15.5% (n = 48) were very confident. Trust in AI companies to use data only for disclosed purposes was modest, averaging 5.55 (SD = 2.52) on a 1–10 scale; 27.5% (n = 85) gave low trust scores (1–4). Confidence in the state was likewise limited: 47.2% (n = 146) did not believe the government currently has enough

Privacy Attitudes and Protective Behaviour

Table 7 presents respondents' attitudinal responses to eight Likert-scale items on a five-point scale from Strongly Agree to Strongly Disagree. The strongest consensus was that AI users need more knowledge and awareness about data privacy, with which 'Agree' and 'Strongly Agree' together accounted for 62.1% (n = 192). At the same time, 50.2% (n = 155) agreed or strongly agreed they would be willing to share confidential work documents with an AI if it saved 10 hours of work per week — a direct behavioural expression of the privacy paradox. Belief that shared information remains exclusively with the company, and that AI technologies have adequate security measures, attracted substantial neutral and agreeing responses, suggesting an over-optimism that may understate real risk.

Table 7. Privacy Attitudes and Protective Behaviour (n (%))

Variable	SA	A	N	D	SD
Consider sensitive data when using AI	55 (17.8%)	106 (34.3%)	107 (34.6%)	30 (9.7%)	11 (3.6%)
Believe info stays exclusively with company	55 (17.8%)	97 (31.4%)	108 (35.0%)	39 (12.6%)	10 (3.2%)
Generative AI might misuse my data	41 (13.3%)	102 (33.0%)	101 (32.7%)	55 (17.8%)	10 (3.2%)
Users need more privacy knowledge/awareness	85 (27.5%)	107 (34.6%)	82 (26.5%)	29 (9.4%)	6 (1.9%)
AI has enough security measures	50 (16.2%)	112 (36.2%)	95 (30.7%)	40 (12.9%)	12 (3.9%)
AI influence on life is positive	47 (15.2%)	113 (36.6%)	107 (34.6%)	36 (11.7%)	6 (1.9%)
Willing to share confidential docs to save 10h/wk	44 (14.2%)	111 (35.9%)	86 (27.8%)	47 (15.2%)	21 (6.8%)
Would seek other sources to validate AI content	42 (13.6%)	104 (33.7%)	101 (32.7%)	45 (14.6%)	17 (5.5%)

Note. SA = Strongly Agree; A = Agree; N = Neutral; D = Disagree; SD = Strongly Disagree.

Bivariate Associations (Chi-Square Analysis)

Table 8 presents cross-tabulations of reading the privacy policy and disclosure of personal information by sex. Reading behaviour did not differ significantly by sex ($\chi^2 = 0.13$, $p = 0.718$), and although a slightly larger proportion of male respondents reported having shared personal information with AI, this difference was not statistically significant ($\chi^2 = 2.48$, $p = 0.115$). Privacy confidence likewise did not differ significantly by sex ($\chi^2 = 2.36$, $p = 0.124$).

Table 8. Privacy Behaviour by Sex (n (%))

Variable	Yes	No
<i>Reads AI privacy policy before use</i>		
Male	112 (48.7%)	118 (51.3%)
Female	41 (51.9%)	38 (48.1%)
<i>Ever shared personal information with AI</i>		
Male	61 (26.5%)	169 (73.5%)
Female	29 (36.7%)	50 (63.3%)

Table 9 presents disclosure of personal information by education level. Disclosure varied

significantly across education levels ($\chi^2 = 12.28$, $p = 0.031$), with the highest proportions of disclosure among PhD and Bachelor-degree respondents and the lowest among primary- and secondary-school respondents. Both reading of privacy policies ($\chi^2 = 22.68$, $p < 0.001$) and confidence in AI privacy ($\chi^2 = 32.37$, $p < 0.001$) also differed significantly by education level, indicating that educational attainment is a key correlate of both awareness and disclosure. Disclosure did not differ significantly by field of study ($\chi^2 = 7.96$, $p = 0.158$).

Table 9. Disclosure of Personal Information by Education Level (n (%))

Variable	Yes	No
Primary School	2 (8.3%)	22 (91.7%)
Secondary School	17 (28.8%)	42 (71.2%)
Diploma	14 (21.5%)	51 (78.5%)
Bachelor Degree	48 (35.6%)	87 (64.4%)
Master Degree	5 (26.3%)	14 (73.7%)
PhD	4 (57.1%)	3 (42.9%)

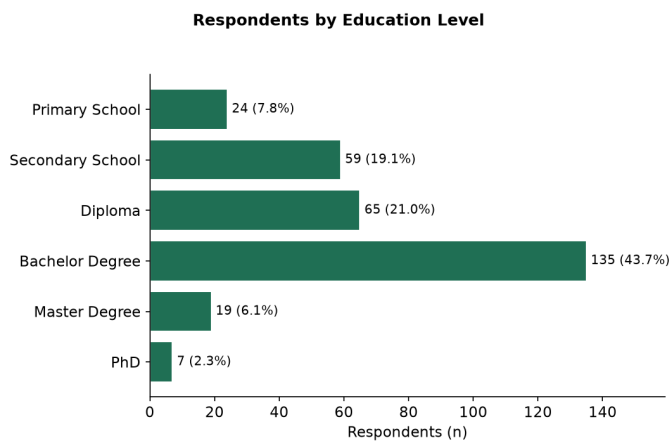


Figure 4. Distribution of respondents by education level.

Discussion

Near-Universal, High-Frequency AI Adoption

The finding that 89.0% of respondents use ChatGPT and 50.8% use AI tools daily places Mogadishu's students firmly within the global wave of generative-AI adoption. This intensity of use is the precondition for cumulative privacy exposure: each interaction is an opportunity for data disclosure, and daily users accumulate exposure rapidly (Dahabiyeh et al., 2026). The dominance of a single platform, ChatGPT, also concentrates risk, since a privacy failure at one provider would affect the overwhelming majority of users.

Disclosure of Sensitive Information and the Exposed Minority

While most sharing was educational or general, the 4.9% ($n = 15$) who reported sharing sensitive financial, health or password data, and the 13.9% sharing work-related information, represent a materially exposed minority. This aligns with industry findings that a non-trivial share of prompts to AI tools contain sensitive data and

that free-tier platforms frequently train on such inputs (Kiteworks, 2024). The contextual-integrity literature warns that the conversational interface lulls users into perceived anonymity, encouraging disclosures they would resist elsewhere (Tran et al., 2025).

The Privacy Paradox in Practice

The data provide a textbook illustration of the privacy paradox (Taddicken, 2014; Hallam & Zanella, 2017). Respondents overwhelmingly agreed that users need more privacy awareness, a majority were not confident about AI privacy, and many noticed evidence of data exploitation through targeted advertising — yet 29.1% had still shared personal information, and a majority would trade confidential documents for time savings. Concern coexists with disclosure, consistent with temporally discounted cost-benefit accounts in which immediate convenience outweighs distant privacy costs (Herbert et al., 2021).

Awareness, Education, and the Trust Deficit

The significant association of education level with privacy-policy reading, disclosure, and confidence (all $p < 0.05$) suggests that awareness scales with educational attainment but, paradoxically, so does disclosure — more-educated, more-confident users share more, echoing findings that greater awareness does not necessarily yield more protective behaviour (Nezhad et al., 2026). Low mean trust in AI companies (5.55/10) and limited confidence in government capacity (47.2% saying the state

lacks sufficient protective power) mirror the institutional-trust deficit documented among students in other developing-country settings (Maguraushe et al., 2026; Masinde et al., 2025).

Implications for Somalia's Data-Protection Architecture

These patterns underscore the importance of operationalising Somalia's Data Protection Act (Law No. 005 of 2023) and its January 2026 implementing regulations (Somalia Data Protection Authority, 2026), and empowering the Data Protection Authority to engage with global AI providers, while embedding data-protection literacy in higher education. Regional coordination through the EAC and continental frameworks could strengthen enforcement leverage that any single national regulator lacks (Prinsloo & Kaliisa, 2022; Issa-Salwe et al., 2024).

Limitations and Future Research

Several limitations should be borne in mind when interpreting these findings. First, the study was confined to Mogadishu, and the sample was recruited on the basis of availability and willingness to participate; it is skewed towards men (74.4%) and Computer Science / IT students (27.5%), so the results should not be generalised to all Somali students or to other regions without caution. Second, all measures are self-reported single items, and disclosure of sensitive information is subject to recall and social-desirability bias; no validated multi-item privacy scale was used and instrument reliability was not estimated. Third, the design is cross-sectional, so

the associations reported describe co-occurrence rather than causation. Fourth, several education-level cells were small (Primary School $n = 24$, Master $n = 19$, PhD $n = 7$), so expected counts below five occurred in the education-level chi-square tests and those results should be read as indicative.

Future research should draw multi-institution and multi-region samples, adopt validated privacy-awareness and self-disclosure instruments, combine self-report with observed behaviour (for example, audits of prompts shared with AI tools), and use longitudinal designs to trace how awareness and disclosure evolve as Somalia's data-protection regime is enforced.

Conclusion

This study provides the first comprehensive empirical examination of awareness and disclosure of sensitive information to AI tools among university students in Mogadishu, Somalia. It documents near-universal adoption of generative AI — led by ChatGPT (89.0%) and used daily by 50.8% — alongside a genuine, if minority, pattern of sensitive-data disclosure (4.9% sharing financial, health or password information) and widespread sharing of personal information (29.1%).

At the same time, the findings reveal a pronounced trust and protection deficit. A majority of respondents lacked confidence in AI privacy (51.1%), trusted AI companies only modestly (mean 5.55/10), and doubted the

government's capacity to protect them (47.2%). The significant variation of awareness and disclosure by education level shows that the problem is not awareness alone but the gap between awareness and protective action — the privacy paradox in a Somali context.

Addressing this gap calls for coordinated action by universities, the National Commission for Higher Education (NCHE), the Ministry of Education, the Data Protection Authority, and regional bodies including the EAC and IGAD, as well as international partners. Embedding data-protection literacy, operationalising national regulation, and building trustworthy institutions are essential to ensure that Somalia's enthusiastic adoption of AI does not come at the cost of its citizens' privacy.

Recommendations

For universities: Integrate AI data-privacy literacy into orientation and digital-skills curricula, with practical guidance on what should never be shared with conversational AI. Train students to read and interpret privacy policies, recognise targeted-advertising signals, and verify AI-generated content against independent sources.

For the government: Operationalise the Data Protection Act (Law No. 005 of 2023) and its 2026 regulations and resource the Data Protection Authority to register and engage major AI and data-processing platforms operating in Somalia. Issue institutional guidance

on the safe use of AI tools in higher education, and mandate baseline data-protection awareness across accredited institutions.

For AI providers and employers: Provide clear, locally accessible privacy disclosures and default privacy-protective settings, especially on free tiers. Employers permitting AI use should establish explicit policies prohibiting the entry of confidential or personally identifiable information into third-party AI tools.

For regional and international partners: Support harmonised data-governance frameworks through the EAC, IGAD and the African Union, and fund digital-literacy and data-protection capacity-building in Somali higher education. Coordinated regional enforcement can provide the leverage that individual national regulators lack against global AI platforms.

References

- Cloud Security Alliance. (2025, April 22). AI and privacy 2024 to 2025: Embracing the future of global legal developments. <https://cloudsecurityalliance.org/blog/2025/04/22/ai-and-privacy-2024-to-2025-embracing-the-future-of-global-legal-developments>
- Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

- Dahabiyeh, L., Taha, N., Thneibat, M., & Bhat, M. A. (2026). Privacy awareness in generative AI: The case of ChatGPT. *Interactive Technology and Smart Education*, 23(1), 25–48. <https://doi.org/10.1108/ITSE-01-2025-0009>
- Federal Republic of Somalia. (2023). Data Protection Act (Law No. 005 of 2023). Somalia Data Protection Authority. <https://dpa.gov.so/about-us/>
- Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68, 217–227. <https://doi.org/10.1016/j.chb.2016.11.033>
- Herbert, C., Marschin, V., Erb, B., Meißner, D., Aufheimer, M., & Bösch, C. (2021). Are you willing to self-disclose for science? Effects of privacy awareness and trust in privacy on self-disclosure of personal and health data in online scientific studies—An experimental study. *Frontiers in Big Data*, 4, Article 763196. <https://doi.org/10.3389/fdata.2021.763196>
- Hirsi, A., & Sharif, A. (2026). Adaptation level of artificial intelligence (AI) in university curriculums: A case study on Mogadishu located universities. *Horn of Africa Journal of Social Science*, 4(Special Issue), 28–34. <https://doi.org/10.70806/ny0mhz54>
- Hussein, A., & Sharif, A. (2025). Assessment of digital skills and training in Somali government institutions. *Horn of Africa Journal of Social Science*, 3(4), 1–9. <https://doi.org/10.70806/jkhtfx87>
- Issa-Salwe, A. M., Baadiyow, A. A., Warsame, A. H., & Osman, A. S. (2024). Integrating Somali higher education with the EAC educational system. *Advances in Social Sciences Research Journal*, 11(8), 114–126. <https://doi.org/10.14738/assrj.118.17386>
- Kelly, S., White, K. M., Kaye, S.-A., & Oviedo-Trespalacios, O. (2025). Tapping into key drivers: Self-disclosure in sensitive health conversations with ChatGPT. *International Journal of Human–Computer Interaction*, 41(24), 15668–15678. <https://doi.org/10.1080/10447318.2025.2499656>
- Kiteworks. (2024). Protecting sensitive data in the age of generative AI: Risks, challenges, and solutions. Kiteworks. <https://www.kiteworks.com/cybersecurity-risk-management/sensitive-data-ai-risks-challenges-solutions/>
- Maguraushe, K., Da Veiga, A., & Martins, N. (2026). Assessing information privacy awareness, expectations, and confidence of students: Evidence from a diagnostic survey in a developing country's higher education sector. *Journal of Cybersecurity and Privacy*, 6(2), 62. <https://doi.org/10.3390/jcp6020062>
- 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>

- Ndiege, J. R. A., & Okello, G. O. (2018). Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya. *African Journal of Information Systems*, 10(3), Article 4.
- Neel, S., & Chang, P. (2023). Privacy issues in large language models: A survey. *arXiv*. <https://arxiv.org/abs/2312.06717>
- Nezhad, M. H., Castro, F. E. V., & Arroyo, I. (2026). Understanding users' privacy reasoning and behaviors during chatbot use to support meaningful agency in privacy. *arXiv*. <https://arxiv.org/abs/2601.18125>
- Prinsloo, P., & Kaliisa, R. (2022). Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. *British Journal of Educational Technology*, 53(4), 894–913. <https://doi.org/10.1111/bjet.13226>
- Somalia Data Protection Authority. (2026, January 5). Council of Ministries approves Data Protection Act Regulations. <https://dpa.gov.so/news/council-of-ministries-approves-data-protection-act-regulations/>
- Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19(2), 248–273. <https://doi.org/10.1111/jcc4.12052>
- Tran, S., Lu, H., Slaughter, I., Herman, B., Dangol, A., Fu, Y., Chen, L., Gebreyohannes, B., Howe, B., Hiniker, A., Weber, N., & Wolfe, R. (2025). Understanding privacy norms around LLM-based chatbots: A contextual integrity perspective. *arXiv*. <https://arxiv.org/abs/2508.06760>
- Ullah, I., Hassan, N., Gill, S. S., Suleiman, B., Ahanger, T. A., Shah, Z., Qadir, J., & Kanhere, S. S. (2024). Privacy preserving large language models: ChatGPT case study based vision and framework. *IET Blockchain*, 4(S1), 706–724. <https://doi.org/10.1049/blc2.12091>
- Yan, B., Li, K., Xu, M., Dong, Y., Zhang, Y., Ren, Z., & Cheng, X. (2024). On protecting the data privacy of large language models (LLMs): A survey. *arXiv*. <https://arxiv.org/abs/2403.05156>