SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 11 | November 2025 - Peer Reviewed Journal

A STUDY OF SOCIAL MEDIA AND FREE AI TOOLS USE AMONG COLLEGE STUDENTS: RISKS, SAFETY STEPS, AND DEVELOPER VIEWS

Mrs. Sneha Vaibhav Chhatre[1], Dr. Sushil Bhimrao Bansode[2]
[1]Assistant Professor, Chintamanrao College of Commerce, Sangli,
[2]Assistant Professor, Chintamanrao College of Commerce, Sangli

ABSTRACT
In India the growth of digital technology had led to an increase in the use of social media and free AI tools, especially among the young generation, college students actively use the platform for education, entertainment, communication, creativity, and other daily activities. However, every digital tool has both advantages and disadvantages. The impact of social media and free AI tools on students depends largely on how they are used. At the same time, issues such as data theft and misuse create certain risks. Therefore, it is important for students to follow safety measures while using digital platform. This study also seeks to understand what specific precautions should be taken, based on the opinion and suggestions of software developers.

KEY WORDS: *Social media, Free AI tools, Safety, College Students, Data Privacy, Online Safety, Viral Trends, Cyber Scams, Developer Views etc.*

1. INTRODUCTIONS

In today's age of information and technology, social media and free AI applications have become an inseparable part of young people's lifestyles. College students, in particular, use these tools not only for entertainment but also for education, communication, creativity, and career development. Platforms like WhatsApp, Instagram, Facebook, and YouTube help students stay connected with people across the world, while free AI applications such as Chat GPT, Google Gemini, Bing AI, and Perplexity make it easier to access information, prepare assignments, conduct research, and develop new ideas.

However, along with these digital conveniences come serious challenges related to data security and privacy. Many students unknowingly share their personal information such as email addresses, mobile numbers, passwords, locations, photos, or academic details across different platforms. As a result, issues like misuse of information, fraud, and identity theft have become increasingly common.

Today, social media is not just a means of entertainment but also a powerful platform for education, career growth, and social connection. Although it is widely used for online study groups, career networking, and content creation, it also has a darker side with risks such as fake news, cyberbullying, phishing attacks, and online fraud. Similarly, while free AI tools provide new opportunities for learning and creativity, they also pose risks related to misinformation, data collection, and privacy breaches.

With the help of AI, human tasks have become faster and more accurate. Yet, if these tools are not used carefully, they can lead to serious problems. Editing photos, creating trending videos, and producing virtual content through free AI tools have become common among youth. But neglecting app security can result in data leaks, hacking, or misuse of personal information.

Therefore, in today's digital era, it is essential for students to use technology wisely and remain aware of data security and privacy. At the same time, app developers must prioritize secure design, data encryption, and user consent to protect users' information.

The main purpose of this study is to understand how college students use social media and free AI applications, identify the risks involved, and explore the measures needed to ensure data safety. By analyzing both students' and developers' perspectives, this research aims to promote awareness and guide society toward safe and responsible digital practices.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 11 | November 2025 - Peer Reviewed Journal

2. STATEMENT OF THE PROBLEM

1. As India becomes more digital college students are using social media and free AI tools more and more. The study checks if they are using these tools in the right and safe way.
2. Students face many problems like scams, data leaks, cyberbullying, and fake news while using social media and free AI tools.
3. Due to risks of data misuse, it is important to find out what safety steps students take and what extra precautions developers suggest to stay safe on these platforms.

3. OBJECTIVES OF THE STUDY

1. To know the usages of social media and AI tools among the students
2. To study the level of awareness, precautions and safety taken by students while using social media and Free AI tools
3. To explore developer views on data privacy risks and recommends safety measures for students using free digital platforms.

4. SCOPE OF THE STUDY

This study looks only at college students in the Miraj area. It checks how they use social media apps like WhatsApp, Instagram, Facebook, and YouTube, and free AI tools like ChatGPT, Google Gemini, Bing AI, Perplexity, and CapCut.
It finds out why they use them for studies, fun, talking to friends, being creative, or making videos and posts.

The study also shows the dangers they face, like data theft, privacy loss, scams, fake messages, bullying, and wrong information. It checks how much students know about these risks and what safety steps they take to protect their phone numbers, emails, photos, and other personal details.

Researcher talked to one software developer to get expert advice. The interview explains how developers keep apps safe using strong locks. safe storage, and clear permission rules. It also shares what developers think students should do to stay safe on free apps.

This research covers only 61 students from Miraj. It does not include students from other places, different age groups, or paid apps. By mixing what students do and what the developer says, this study gives easy tips to help everyone use social media and AI tools safely.

5. RESEARCH METHODOLOGY

1. Research design

The study is descriptive in nature. It describes the daily habits of college students when using social media and free AI tools like which apps they open, how much time they spend, and why they use them. It also explores the risks they face and the safety steps they take. At the same time, it digs deeper into expert views to find practical solutions.

2. Study area and Sampling

The population includes all college students studying in the Miraj region. From this group, a sample of 61 students was selected. These students were chosen using simple random sampling, meaning every student in Miraj colleges had an equal chance of being picked. This was done by visiting different colleges and asking students to fill out the form. Additionally, one experienced software and app developer was selected for an interview to get professional insights.

3. Data Collection Method

All data in this study is fresh and collected directly forom the respondent i.e this study is based on primary data. This data is collected from:

- **For Students**: A structured questionnaire was used. It had clear, closed-ended questions. The questions asked about age, gender, favorite apps, time spent online, reasons for use, safety habits, experience with scams, and awareness about privacy. The form was given in person to 61 students, and they filled it out on the spot.
- **For the Developer**: A short semi-structured interview was conducted. This means a list of 10 key questions was prepared, but the developer was free to explain in detail. Questions covered topics like how apps are made secure, risks of free tools, what students should avoid, and what developers must do to protect user data.

No old books, websites, or reports were used. All information comes from the students and the developer.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 11 | November 2025 - Peer Reviewed Journal

4. Limitations

This study has a few limits:

a) Only 61 students were surveyed, so results may not represent all students in India.
b) Just one developer was interviewed other experts could give a wider view.
c) The study is limited to Miraj only**.** Habits and risks may differ in big cities or villages.

6. DATA ANALYSIS

Table no. 1
Demographic Profile of students

Sr. No.	Particulars	Category	Number	Percentage
1	Age of Students	18–20 years	49	80.30%
		21–22 years	6	9.80%
		23–25 years	6	9.90%
2	Education	Graduation	48	78.20%
		Post-Graduation	4	6.60%
		Short-term Courses	9	15.20%
3	Gender	Male	30	49.18%
		Female	31	50.82%
4	Area	Rural	26	42.62%
		Urban	35	57.38%
	Total		**61**	**100%**

(**Sources:** Primary data)

From the above tables, it is seen that most of the respondents (80.3%) belong to the age group of 18–20 years. The percentage of respondents in the 21–22 and 23–25 age groups is comparatively low, around 9.8% to 9.9%.In terms of educational qualification, a large number of respondents (78.2%) are at the graduation level. Around 11.8% have completed post-graduation, while 10% are pursuing short-term or professional courses. Out of 61 students,31 students are male and 30 students are female. Also 26 students are from rural area and 35 students are from urban area.

Table No. 2
Students' Awareness and Usage of Social Media & Free AI Tools

Sr. No.	Particular	Category	Frequency	Percentage
1	Most Used Social Media	WhatsApp	24	39.3%
		Instagram	23	37.7%
		YouTube	9	14.8%
		Facebook	4	6.6%
		Others	1	1.6%
2	Daily Time Spent on Social Media	1–2 hours	22	36.1%
		2–3 hours	30	49.2%
		3–5 hours	9	14.8%
3	Participation in Viral Trends	Always	9	14.8%
		Sometimes	11	18.0%
		Rarely	17	27.9%
		Never	24	39.3%
4	Most Used Free AI Tool	ChatGPT	32	52.5%
		CapCut	7	11.5%
		Others	22	36.1%
		Education	27	44.3%
		Entertainment	16	26.2%

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 11 | November 2025 - Peer Reviewed Journal

5	**Main Purpose of Use**	Content Creation	12	19.7%
		Popularity	6	9.8%
6	**Reading Privacy Policy**	Always	21	34.4%
		Sometimes	15	24.6%
		Rarely	4	6.6%
		Never	21	34.4%
7	**Experience with Scams**	Yes, Faced Scam	17	27.9%
		No	44	72.1%
8	**Level of Concern About Data Privacy**	Not Concerned	20	32.8%
		Moderately Concerned	10	16.4%
		Highly Concerned	5	8.2%
		No Response	26	42.6%
9	**Perceived Risk in Viral Trends**	Yes, Perceive Risk	18	29.5%
		No, Do Not Perceive Risk	25	41.0%
		Not Sure	18	29.5%
10	**Data Privacy vs Popularity**	Data Safety	40	65.6%
		Popularity	7	11.5%
		Both Important	14	23.0%
11	**Taking Safety Measures**	Yes, Regularly	37	60.7%
		Sometimes	10	16.4%
		Rarely	11	18.0%
		Never	3	4.9%

(Source: Primary data**)**

The survey of 61 college students from Miraj shows clear patterns in how they use digital tools. WhatsApp is the most popular social media app, used by 24 students (39.3%)**,** closely followed by Instagram with 23 students (37.7%)**.** YouTube comes third with 9 students (14.8%), while Facebook and other platforms are used by only 4 (6.6%) and 1 (1.6%) student respectively. This means nearly 77% of students mainly use WhatsApp and Instagram to stay connected.

On average, students spend 2–3 hours daily on social media 30 students (49.2%)**,** while 22 students (36.1%) spend 1–2 hours, and 9 (14.8%) spend 3–5 hours. So, almost half the group uses social media for 2–3 hours every day.

When it comes to viral trends, most students stay away: 24 (39.3%) never participate, 17 (27.9%) do it rarely**,** 11 (18.0%) sometimes**,** and only 9 (14.8%) always join. This shows over 67% avoid or rarely follow trends.

Among free AI tools, ChatGPT is the clear leader with 32 students (52.5%) using it most, followed by CapCut with 7 (11.5%)**,** and 22 students (36.1%) using other AI tools. The main reason for using these tools is education 27 students (44.3%) use them for studies, notes, or assignments. Entertainment comes next with 16 (26.2%), then content creation **(**12, 19.7%**),** and gaining popularity **(**6, 9.8%**).**

However, privacy habits are weak**:** 21 students (34.4%) always read privacy policies**,** 15 (24.6%) sometimes**,** 4 (6.6%) rarely, and 21 (34.4%) never read them. This means over 40% either rarely or never check what apps do with their data.

About 17 students (27.9%) have faced online scams or fake profiles, while 44 (72.1%) have not. On data privacy concern**,** 20 (32.8%) are not worried**,** 10 (16.4%) are moderately concerned**,** 5 (8.2%) are highly concerned, and a large 26 (42.6%) gave no response showing low overall awareness.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 11 | November 2025 - Peer Reviewed Journal

Only 18 students (29.5%) see risk in viral trends, 25 (41.0%) do not, and 18 (29.5%) are not sure. But when asked to choose, 40 students (65.6%) say data safety **is** more important than popularity, 14 (23.0%) want both, and only 7 (11.5%) pick popularity.

Finally, 37 students (60.7%) regularly take safety steps**,** 10 (16.4%) sometimes**,** 11 (18.0%) rarely, and 3 (4.9%) never meaning over 95% try to stay safe at least sometimes.

In short the Students heavily use WhatsApp, Instagram, and ChatGPT for studies and fun**,** spend 2–3 hours daily, and mostly avoid viral trends. But many skip privacy policies**,** few are highly concerned, and over 40% don't see risks even though 1 in 4 has faced a scam. Still, most value data safety and try to follow safety steps. This shows good intentions but weak awareness a clear need for better digital safety education.

Table No. 3
Developer's Views on Data Privacy and Safety Measures

Particular	Agree	Strongly Agree	Neutral	disagree	Strongly disagree
Free AI Application more risky than paid apps in terms of data privacy			✓		
Free AI Application usually involve hidden data mining and unauthorized data sharing			✓		
Students should avoid sharing personal data (Phone number, email, Photos)on free apps	✓				
Checking permission before installations is an important Precautions		✓			
Using strong authentication methods (two factor authentications) reduce chance of data leakage		✓			
Developers should design apps with security like encryption and secure server storage		✓			
If data leakage happens, students should immediately change passwords and uninstall the suspicious app		✓			
Reporting data leakage to cyber cell or concered authority is essential		✓			
Following social media trends(Reels, Filters, Viral Challenges)increasing the chance of data leakage		✓			
Students should avoid participating in viral trends that require unnecessary access to personal data		✓			

(Source: Primary data**)**

The developer strongly agrees with every statement in Table No. 3. Free AI apps are more risky than paid ones due to hidden data mining and unauthorized sharing. Students must avoid sharing personal details, always check permissions, and use two-factor authentication. Developers should build apps with encryption and secure storage. In case of a leak, students need to change passwords, uninstall the app, and report to cyber cell. Viral trends increase data risks, so students should skip those asking for extra access. Overall, the developer sees free apps as unsafe and calls for strict student habits and strong app design.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 11 | November 2025 - Peer Reviewed Journal

7. FINDINGS

1. Among the 61 students surveyed, 24 (39.3%) use WhatsApp as their primary social media platform, while 23 (37.7%) prefer Instagram, making these two apps the most widely used for daily communication and social interaction.
2. Nearly half of the students 30 (49.2%**)** spend 2 to 3 hours daily on social media, followed by 22 (36.1%) spending 1 to 2 hours, indicating a balanced yet significant engagement with digital platforms.
3. 32 students (52.5%) report ChatGPT as their most-used free AI tool, showing its strong acceptance for academic support, idea generation, and content creation among college youth.
4. The main reason for using social media and AI tools is education 27 students (44.3%) use them for assignments, notes, research, and study groups, proving digital tools are now part of learning.
5. A large majority 24, (39.3%**)** never participate in viral trends, and 17 (27.9%) do so rarely. This shows most students avoid risky online challenges, possibly due to awareness or lack of interest.
6. 21 students (34.4%) never read privacy policies**,** and another 21 (34.4%) always do, revealing a sharp divide over one-third ignore critical legal information about data use.
7. Although 17 students (27.9%) have faced scams or fake accounts, 44 (72.1%) have not. Yet, 41% still believe viral trends are safe, showing a gap between experience and caution.
8. Only 5 students (8.2%) are highly concerned about data privacy, 10 (16.4%) are moderately worried, 20 (32.8%) are not concerned, and 26 (42.6%) gave no response indicating alarmingly low awareness.
9. When forced to choose, 40 students (65.6%) say data safety is more important than online popularity**,** and 14 (23.0%) want both, showing maturity in long-term thinking.
10. 37 students (60.7%) regularly take safety steps like using strong passwords, avoiding suspicious links, or limiting app access. Only 3 (4.9%) never do, meaning over 95% try to protect themselves at least sometimes.

8. SUGGESTIONS

1. Organize monthly workshops where experts teach students how to spot fake profiles, phishing links, and unsafe apps using live demos.
2. Include a short quiz on app privacy rules in college orientation programs so every new student learns to read terms before installing apps.
3. Create a safe app list for Students, colleges should publish a verified list of trusted free AI and social media tools with clear safety ratings to guide safe usage.
4. Teach Two Factor Authentication (2FA), run hands-on sessions showing how to enable 2FA on WhatsApp, Instagram, and email a simple step that blocks most hacking attempts.
5. Develop a Mobile Safety Checklist: Distribute a pocket-sized card or sticker with 5 key rules: Check permissions, Use strong passwords, Avoid unknown links, Never share OTP, Report fake accounts
6. Train responsible students to help classmates set up privacy settings, remove risky apps, and report threats.
7. Use college notice boards and WhatsApp groups to share real scam stories from trends that asked for camera, location, or contact access.
8. Teach students to change passwords, uninstall suspicious apps, and inform college IT cell the moment they suspect a breach.
9. Students and colleges should demand clear permission pop-ups and data use summaries in free apps before installation.
10. Add a 2-credit course on “Digital Citizenship & Safety” covering privacy laws, ethical AI use, and online behavior.
11. Create a college WhatsApp number or email where students can quickly report scams, data leaks, or cyberbullying for fast support.
12. Organize a monthly event where students review their phones, delete old or unused apps, and free up space while reducing data risk.

9. REFERENCES

1. *Boyd, D. (2014).* It’s complicated: The social lives of networked teens. *Yale University Press.*
2. *Data Security Council of India. (2024).* Cyber safety handbook for students. *https://www.dsci.in*
3. *Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., ... & Williams, M. D. (2023). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy.* International Journal of Information Management, 66, *102–114. https://doi.org/10.1016/j.ijinfomgt.2021.102114*
4. *Google Safety Center. (2025).* How to stay safe online: Tips for students. *https://safety.google/students*

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 11 | November 2025 - Peer Reviewed Journal

5. *Government of India. (2023).* The Digital Personal Data Protection Act, 2023. *Ministry of Electronics and Information Technology. https://www.meity.gov.in/content/digital-personal-data-protection-act-2023*
6. *Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2021). Advances in social media research: Past, present and future.* Information Systems Frontiers, 23*(1), 1–28. https://doi.org/10.1007/s10796-020-10065-9*
7. *National Cyber Crime Reporting Portal. (2025).* Guidelines on reporting online fraud and data breaches. *https://cybercrime.gov.in*