SOUTH AFRICAN YOUNG PEOPLE'S

PERSPECTIVES ON DIGITAL PRIVACY

Nov 2024

MEDIA MONITORING AFRICA

Media Monitoring Africa (MMA) was founded in 1993 and is located in Johannesburg, South Africa. Our mission is to champion ethical journalism that upholds human rights, fostering an environment where both media and influential entities honour human rights while advancing democracy and the principles of justice and fairness. Leveraging technology, social media, and data tools, MMA implements effective media strategies for impactful change.

Suite No.2, Art Centre,
22 6th St, Parkhurst,
Johannesburg, 2193
South Africa
info@mma.org.za

With thanks to Reset.Tech Australia for support with the research.

With thanks to the Internet Society Foundation supporting the research.

Internet Society Foundation

Summary

We spoke to 24 young people aged 13–17 in Johannesburg and surveyed 60 more from across South Africa to discover their views on privacy and trust in this digital age. The aim was to explore what young people think privacy in a digital age looks like and the ‘rules’ they would like in place to help realise this.

It was found that young people hold complex views on what privacy means in a digital age. The 24 young people involved in an in-person workshop described privacy as having 5 key aspects:

1. Privacy is seen as a human right and a privilege that everyone should enjoy.
2. Privacy is the freedom to be yourself without intrusions from others.
3. Privacy enables personal boundaries that give control.
4. Privacy enables relationships we can control, including how much we want to see others and how much we want to be seen by others.
5. Privacy gives young people safety, security and comfort.

‘Privacy is the right to be free and to have personal boundaries, especially in our relationships with others, that we can control. It gives us safety, security and comfort.’

Young people also had complicated views about whether they enjoyed privacy online. A survey of 60 young people found that few trusted their personal information was handled carefully online, and around half did not feel their privacy was respected by digital services.

Young people expressed strong views about what should be done to improve their privacy online. Specifically, they described seven key areas for improvement:

1. More control over data, including more meaningful consent about what data is collected and how it is used, as well as more options to delete it easily.
2. Greater transparency and awareness about data collection and use, with clearer and more meaningful explanations. They felt that privacy policies were often vague and unclear, preventing a true understanding of how their data was collected and used.
3. Enhanced security measures, such as better password protection, encryption and regular prompts to review security settings. They also wanted specific protections from hackers, catfishers and scammers.
4. Limitations on data sharing, such as not sharing data with third parties or preventing data from being ‘sold’ for advertising or when companies are bought. This included wanting less data broadcast about them in general.
5. Reduced online ‘tracking’, such as not tracking app usage or browsing history, particularly sensitive personal data like biometric and location data.
6. Automatic data deletion, ensuring that personal data is deleted regularly when it is no longer needed.
7. Less data collection overall, especially for those under 18. Suggestions included only collecting essential data and avoiding data collection from under-18s whenever possible.

Contents

Introduction

Globally, children and young people under 18 years old make up a third of the world's online users, and they use a range of digital technologies and services.[1] Virtually all of these services, from EdTech products to smartphones to popular apps like Instagram and WhatsApp, collect a trove of personal information about young people. This digital world relentlessly collects, collates and analyses data about the children who use these products, from phone ID numbers to GPS locations to the contents of their emails. Young people in South Africa are no exception to this global trend.

This means that children growing up in South Africa today create a data footprint that would have been unimaginable even a decade ago, with children and young people now being 'datafied' from birth.[2]The best available estimate of how many data points have been collected about each child by their 13th birthday is 72 million.[3]

This situation has implications for young people's privacy. Under the Convention on the Rights of the Child[4] and the African Charter on the Rights and Welfare of the Child,[5] children have the right to be free from arbitrary interference with their privacy. Extensive data footprints may pose a risk to this right. Children and young people also have the right to be heard on matters that affect them.[6]

This research set out with a simple aim: to explore what children and young people think about their online privacy, whether they trust the technology that collects their data and what, if anything, they want done to improve their privacy online.

The research involved workshops and surveys with young people exploring their perspectives. These were held in October 2024, supported by the Internet Society Foundation. Similar workshops and surveys were conducted in Ghana, Antigua and Barbuda, Australia and Slovenia. This report focuses on the South African perspectives and considers their implications for privacy policy in the country.

The aim is to contribute to a rich debate about the need for better privacy protections in South Africa and across Africa and to ensure that children and young people are included in these discussions. We hope that their perspectives and experiences spur a greater focus on creating a digital world where children can grow up safely and privately.

[1] Sonia Livingstone, John Carr, and Jasmina Byrne 2015. *One in Three: The Task for Global Internet Governance in Addressing Children's Rights. Global Commission on Internet Governance*: https://www.cigionline.org/sites/default/files/no22_2.pdf

[2] Veronica Barassi (2020) *Child | Data | Citizen* MIT Press, London

[3] In New Economics Foundation (2020) *iSpy* https://neweconomics.org/uploads/files/i-Spy__NEF.pdf

[4] Article 16 UN General Assembly (1989) *Convention on the Rights of the Child General Assembly resolution 44/25*

[5] Article 10 African Union Ordinary Assembly (1990) *African Charter on the Rights and Welfare of the Child*

[6] Article 12 in the UN General Assembly (1989) *Convention on the Rights of the Child General Assembly resolution 44/25* and when it comes to their right to be heard in administrative issues such as the development of privacy policies, Article 4 African Union Ordinary Assembly (1990) *African Charter on the Rights and Welfare of the Child*

Research methods

This research involved a focus group with 24 young people aged 13–17 years old in Johannesburg. The young people were recruited from schools across Johannesburg. They were all keen digital users, expressing a love for apps and digital services like Spotify, Pinterest, TikTok, YouTube and online multiplayer games.

They undertook three guided activities:

1. Discussing and exploring their data footprint in the digital age, including who has access to their data and how comfortable they feel about this.
2. Engaging in group work to develop a core idea of what privacy means to young people in South Africa in 2024.
3. Creating a list of 'dos and don'ts' for their data or suggestions for policymakers about rules that could govern data use.

This was supplemented by a survey of 60 additional young people aged 13–17 years old, which was conducted through schools across the country.

Comparable workshops and surveys were held with young people in Ghana, Antigua and Barbuda, Australia and Slovenia in 2022 as part of an international research effort.[7]

[7] More information about the research can be found TrustTech4Kids 2024 *Homepage* https://trustech4kids.github.io/

Findings

What does privacy online mean for young people?

One of the first activities in the workshops was to develop a group definition of privacy online. As we discussed young people's experiences in the digital age, along with their expectations of privacy, it became clear that the participants had a nuanced and contextual understanding of privacy in the digital age.

Five key aspects of online privacy emerged in the workshop:

1. Privacy is seen as a human right and a privilege that everyone should enjoy.
2. Privacy is the freedom to be yourself without intrusions from others.
3. Privacy enables personal boundaries that give control.
4. Privacy enables relationships we can control, including how much we want to see others and how much we want to be seen by others.
5. Privacy gives young people safety, security and comfort.

When the group worked together to develop a collective definition, they described privacy as:

'Privacy is the right to be free and to have personal boundaries, especially in our relationships with others, that we can control. It gives us safety, security and comfort.'

Do young people feel their privacy is respected online?

We explored whether young people felt their privacy was respected and if they trusted that their sensitive personal information was handled carefully in an online survey.

We found that young people largely did not trust digital products to handle their information carefully (see Figure 1):

- Only a quarter of respondents (25%) trusted digital services to handle their data carefully. They described trust as arising partly from the normalisation and scale of these products (e.g. 'because they have information about lots of people') and from their commitments to data protection (e.g. 'because they always promise us they will keep it safe').
- The largest proportion, 42%, did not trust digital services to handle their data carefully. Young people expressed their lack of trust in platforms due to a lack of clarity about what data is being processed: e.g. 'the reason why I do not trust them is because I don't know what they do with my data and why they need my data.' They also mentioned a lack of control, stating, for example 'They have the power or authority to do as they please with my data.'
- A large portion of respondents (29%) neither trusted nor distrusted platforms and spoke about having ambivalent feelings about their data: e.g. 'I think I feel this way because although they do reassure us that they keep our personal information private, that might not completely be true. But since we have no way of confirming this, then I can't say whether I trust or distrust them.'

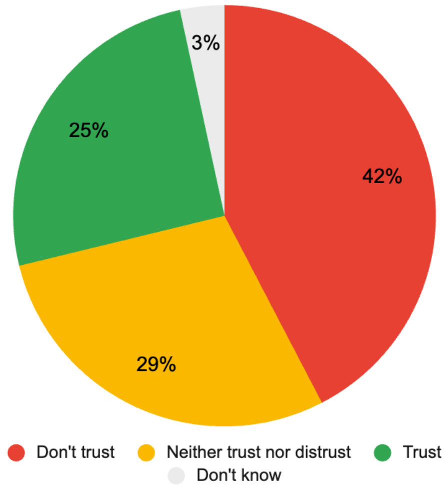


Figure 1: Responses to the question 'Digital products, like TikTok, YouTube and Whatsapp, collect a lot of data and information about people who use them. Do you trust them to handle your information carefully?' n= 59

However, when we asked the respondents if they felt that digital platforms respected their privacy, a slightly more positive picture emerged (see Figure 2).

- Nearly half (48%) said they felt digital services respected their privacy.
- One in five young people (20%) said they did not feel their privacy was respected.
- Nearly a third (31%) felt their privacy was neither respected nor disrespected.

Curiously, young people felt more positively about their privacy being respected than about their data being handled carefully. Their suggestions for what might make them feel more 'private' online suggest a range of reasons for this discrepancy. Regardless, there is still a significant issue: half of young people do not unequivocally feel their privacy is respected online.

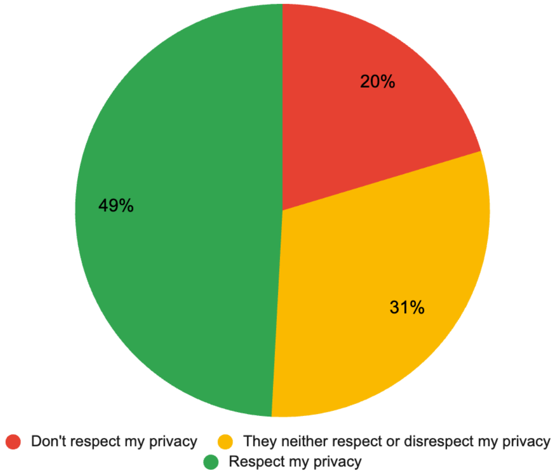


Figure 2: Responses to the question 'In your opinion, when thinking about whether digital products respect your privacy, (which statement do you agree with)?' n= 59

What do young people want to feel private online?

We asked both in the survey and the workshops what young people thought the ‘rules should be online’ to help them feel more private.

In the survey, young people suggested a range of ways that might encourage a stronger sense of privacy online. Their responses reflected a desire for control, transparency and a more rights-respecting digital environment overall. This may help explain why survey participants had mixed feelings about whether their privacy was respected. Young people’s desires for more control and transparency may influence their perception of privacy online.

We asked young people to select from a set list of options regarding what might help improve trust in digital products (see Figure 3).

What, if anything, would make you trust digital products more with your privacy? (n = 55)	
If products offered you more control about what information they could collect and what they could do with it	33%
If products were clearer about what personal information they were collecting and how they were using it	29%
If products agreed to respect your rights in general	20%
If products only used your information in ways that you had signed up for, not for other purposes	11%
If products offered easy ways to complain or fix a problem if something went wrong	7%
If products did not sell your information	2%
If products did not target you with personalised ads	4%

Figure 3: Responses to the question ‘What, if anything, would make you trust digital products more with your privacy? (Select as many as you think would help)’ (n = 55).

We also asked survey respondents for their ideas in an open-ended way and received a wide range of responses, including:

- Responses expressing a desire for age-appropriate content or contacts (‘When the content aligns with my age group’, ‘By making sure young people are not exposed to adult-rated websites’, ‘I would feel safer if the platform only connected me with content and users of the same age as me’, etc.).
- Stronger commitments to data security (‘If they would often send me proof that my information is secured and/or they communicated with me every 48 hours to notify me about my personal information’, ‘I think it would be when my account cannot be hacked’, ‘Security systems in the digital world could make me feel private because, with security systems, personal information is protected at all costs’).
- Stronger laws (‘If the laws are strict’, ‘If they improve the laws that should protect our digital world’, ‘More enforced laws’).

In the workshop, the discussion around how young people want to feel private online replaced the development of a list of ‘dos and don’ts’ for privacy. These have been included in full in the appendix but are clustered around seven areas:

1. More control over data, including more meaningful consent about what data is collected and how it is used, as well as more options to delete it easily.
2. Greater transparency and awareness about data collection and use, with clearer and more meaningful explanations. They felt that privacy policies were often vague and unclear, preventing a true understanding of how their data was collected and used.
3. Enhanced security measures, such as better password protection, encryption and regular prompts to review security settings. They also wanted specific protections from hackers, catfishers and scammers.
4. Limitations on data sharing, such as not sharing data with third parties or preventing data from being 'sold' for advertising or when companies are bought. This included wanting less data broadcast about them in general.
5. Reduced online 'tracking', such as not tracking app usage or browsing history, particularly sensitive personal data like biometric and location data.
6. Automatic data deletion, ensuring that personal data is deleted regularly when it is no longer needed.
7. Less data collection overall, especially for those under 18. Suggestions included only collecting essential data and avoiding data collection from under-18s whenever possible

Both methods aligned in their agreements on wanting more control and transparency regarding their data use.

Recommendations

The young people involved in the workshops wanted to communicate their list of privacy principles to a range of decision-makers to ensure their voices were heard. These included:

- Data regulators and data protection decision-makers, both in South Africa and Internationally
- Social media companies such as Meta, Google, TikTok and Pinterest
- The minister of education
- The minister of information
- Community groups who work on children's rights

Beyond this, the ideas about privacy and potential rules to follow could help inform and strengthen debates about privacy laws and policies within South Africa. Specifically, it raises the urgent need for more awareness and work around ensuring children's data privacy in South Africa. Furthermore, it highlights the potential of, and the need to, engage with more children on these issues.

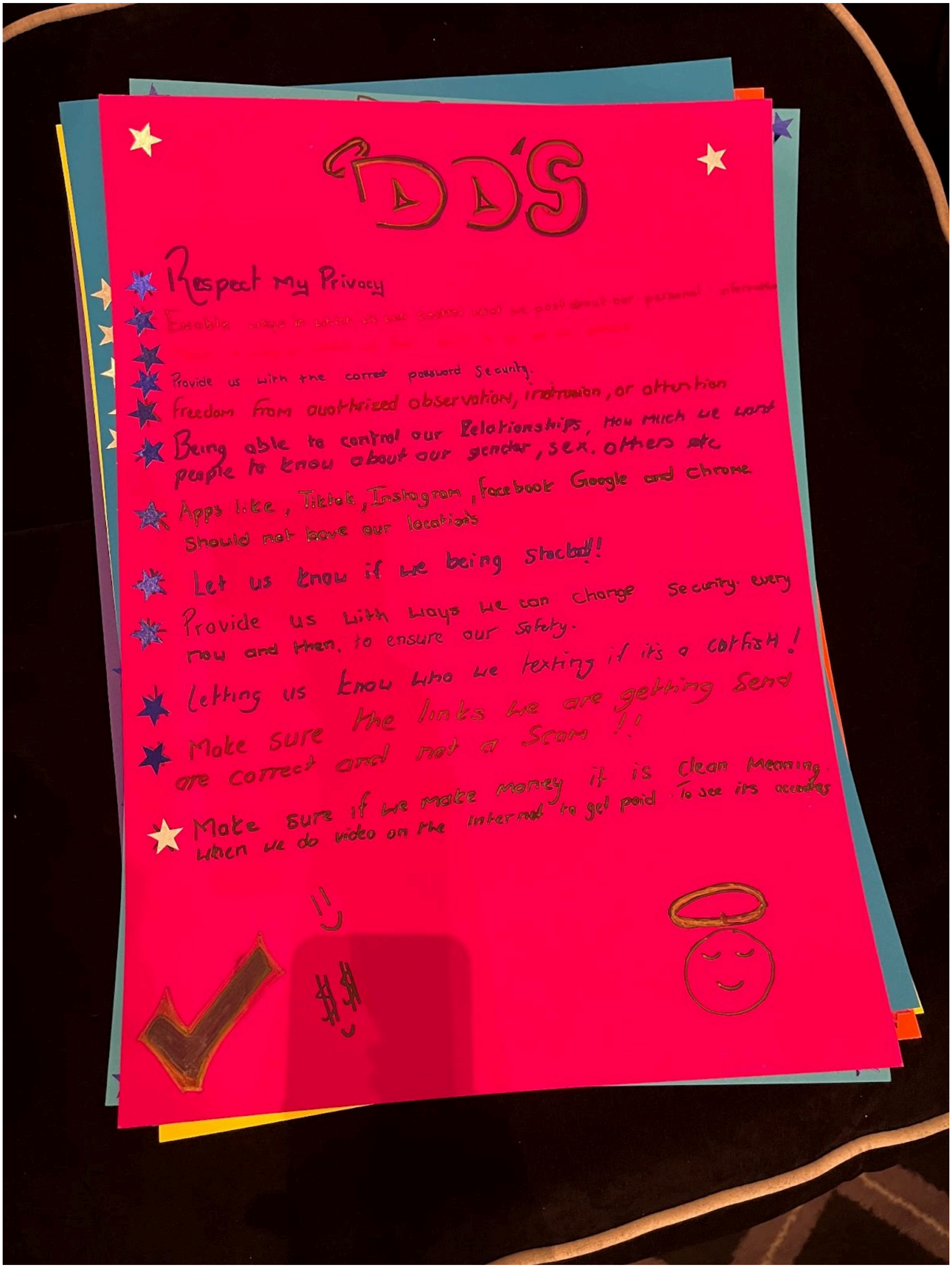
Children's privacy online is everybody's business, and we urge everyone to reflect on the key messages young people have shared and to consider how they might be able to advance children's right to privacy in the online world.

Appendix 1: Dos and don’ts from the workshops

Dos	*Don’ts*
Respect my privacy Enable ways in which we can control what we post about our personal information Make a way in which we feel safe to do as we please Provide us with the correct password security Freedom from authorized observation, intrusion or attention Being able to control our relationships, how much we want people to know about our gender, sec, others etc Apps like TikTok, Instagram, Facebook, Google and Chrome should not have our location Let us know if we are being stalked Provide us with ways we can change security every now and then, to ensure our safety Letting us know who we are texting if it’s a catfish Make sure the links we are getting sent are correct and not a scam Make sure if we make money its clean meaning when we do video on the internet to get paid to see it’s accounts	I don’t want my data shared with third party companies Don’t want my data targeted for ads Don’t want my data stored on other services Don’t want my data analyzed for research Don’t want my data to be distributed to other organizations Don’t want them to track my online actives
Save details for future purposes Delete my data when no longer needed Ensure my safety when logging in Notify me about data incidents Protect my date with strong passwords I want options to delete my data	Do not record me at all times Do not track my activities Do not display my data to the public Do not access my other apps on my device Do not ask me for confidential information Do not require any sensitive information when signing up for products

Please do! Human right Sensitivity Ask in questions or survey Do not invade Awareness Privacy!!! Secure! Personal bubble Trust	Do not share my personal information without me knowing Do not use my personal information for your own benefit. For example, do not use my name and/or number when advertising Do not throw away my personal information without reassuring me Do not access my personal information without my permission Do not sell my personal data to other parties
Do give an option to save personal data Do alert the user if info needs to be shared Do have an option to delete personal data Do keep personal information safe Do teach users how to keep information safe Do have security check-ups in a certain period of time Do delete my information when selling the app	I do not want my biometric data such as height, weight and facial structure to be taken/ collected by companies as these things separate me from the rest and the idea of someone collecting my data seems oppressive I do not want the data such as my location to be accessed. Companies that do this dehumanize us and see us as numbers and mere statistics, I do not see the purpose of knowing a teenagers location as ethical Applications that do not encrypt messages between two parties are depriving people the right to express themselves, knowing that the interactions we have as people are not seen as sacred might make others feel like social media is pointless I do not want the sata such as my banking details, photos or videos to be accessed by any random ware, spyware and malware We should normalize the protection of children Some data is too sacred to share Let kids be kids not numbers, stats or anything else, just kids

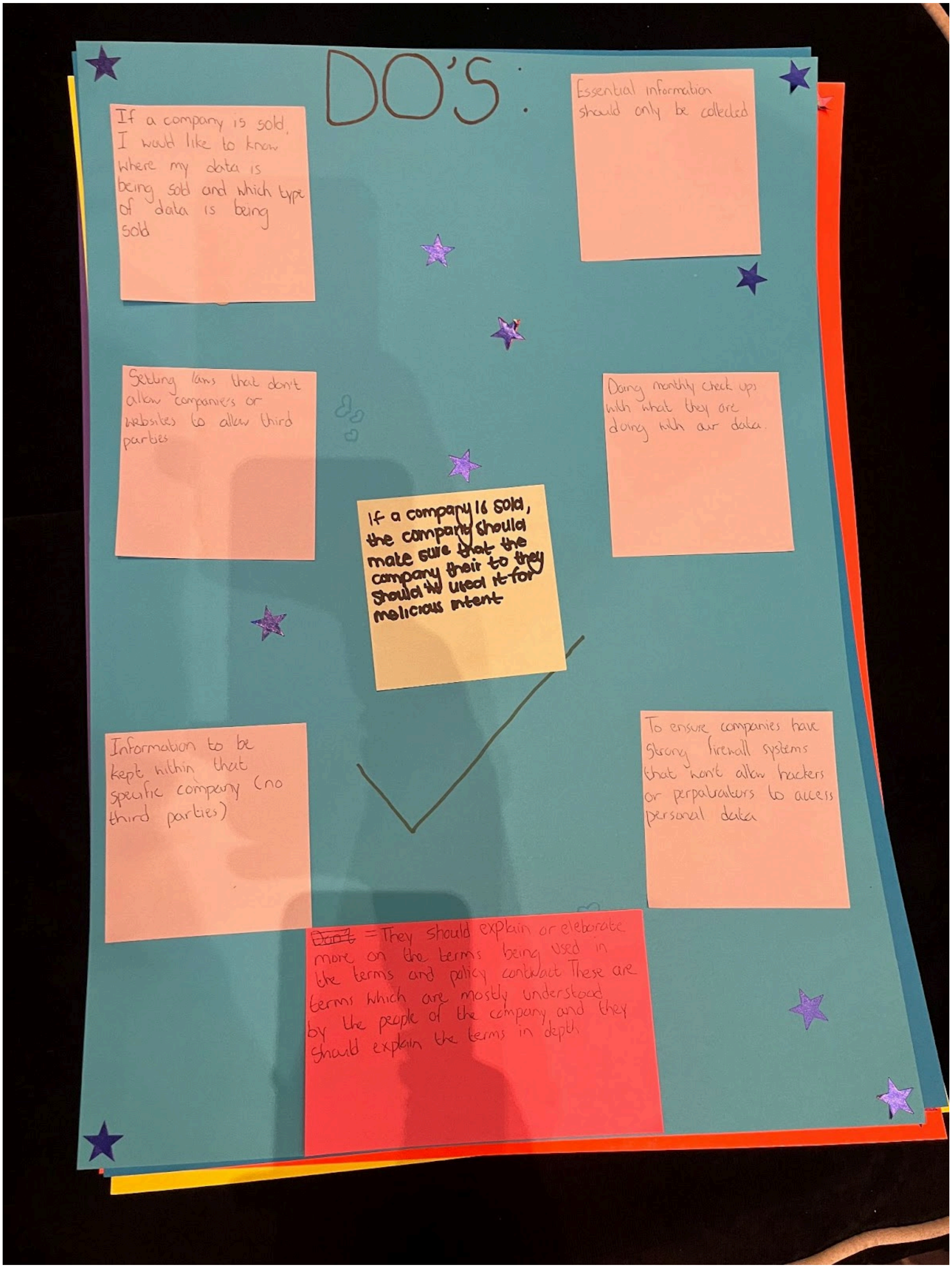
If a company is sold I would like to know where my data is being sold and which type of data is being sold Essential information should only be collected Setting laws that don't allow companies or websites to allow third parties (access to data) Doing monthly check ups with what they are doing with our data If a company is sold, make sure that the company they're (sold) to they shouldn't use it for malicious intent Information to be kept within that specific company (no third parties) To ensure companies have strong firewalls systems that don't allow hackers or perpetrators to access personal data They should try to explain or elaborate more on the terms being used in the terms and policy contract. These are by the people of the company and they should explain the terms in depth	No third parties involves Not to keep the data after its use Not to collect the data of minors Blocking unsecure apps/websites from being easily accessed Do not use data for anything other than the services being provided Giving less vague definitions of how your data will be used (in policies) To not store information with companies/websites especially if they have unknown intentions
Inform the users if there are any changes with the app Apply proper security measures Protect your information from hackers or spams Use location information for the safety of the user Temporary storage of one's personal information	Leakage of personal information Storage of one's personal information for a long period of time Invasion of personal data without owner's consent Unnecessary usage of one's personal data Usage of one's personal info/data in pretendance of another personal (plagiarism) Violation of one's basic human right to privacy and security (generalism) In conclusion, infringing or violating one's basic right to privacy in any way should be considered as a don't or illegal act



DD'S

- Respect My Privacy
- Enable ways in which we can control what we post about our personal information
- [illegible]
- Provide us with the correct password Security.
- freedom from auothrized observation, instrusion, or attention
- Being able to control our Relationships, How much we want people to know about our gender, sex. others etc
- Apps like, Tiktok, Instagram, facebook Google and chrome should not have our location's
- Let us know if we being stocked!
- Provide us with ways we can change security every now and then. to ensure our safety.
- letting us know who we texting if it's a catfish!
- Make sure the links we are getting send are correct and not a Scam !!
- Make sure if we make money it is clean Meaning when we do video on the internet to get paid. To see its accurates

$$



DO'S:

If a company is sold, I would like to know where my data is being sold and which type of data is being sold

Essential information should only be collected

Setting laws that don't allow companies or websites to allow third parties

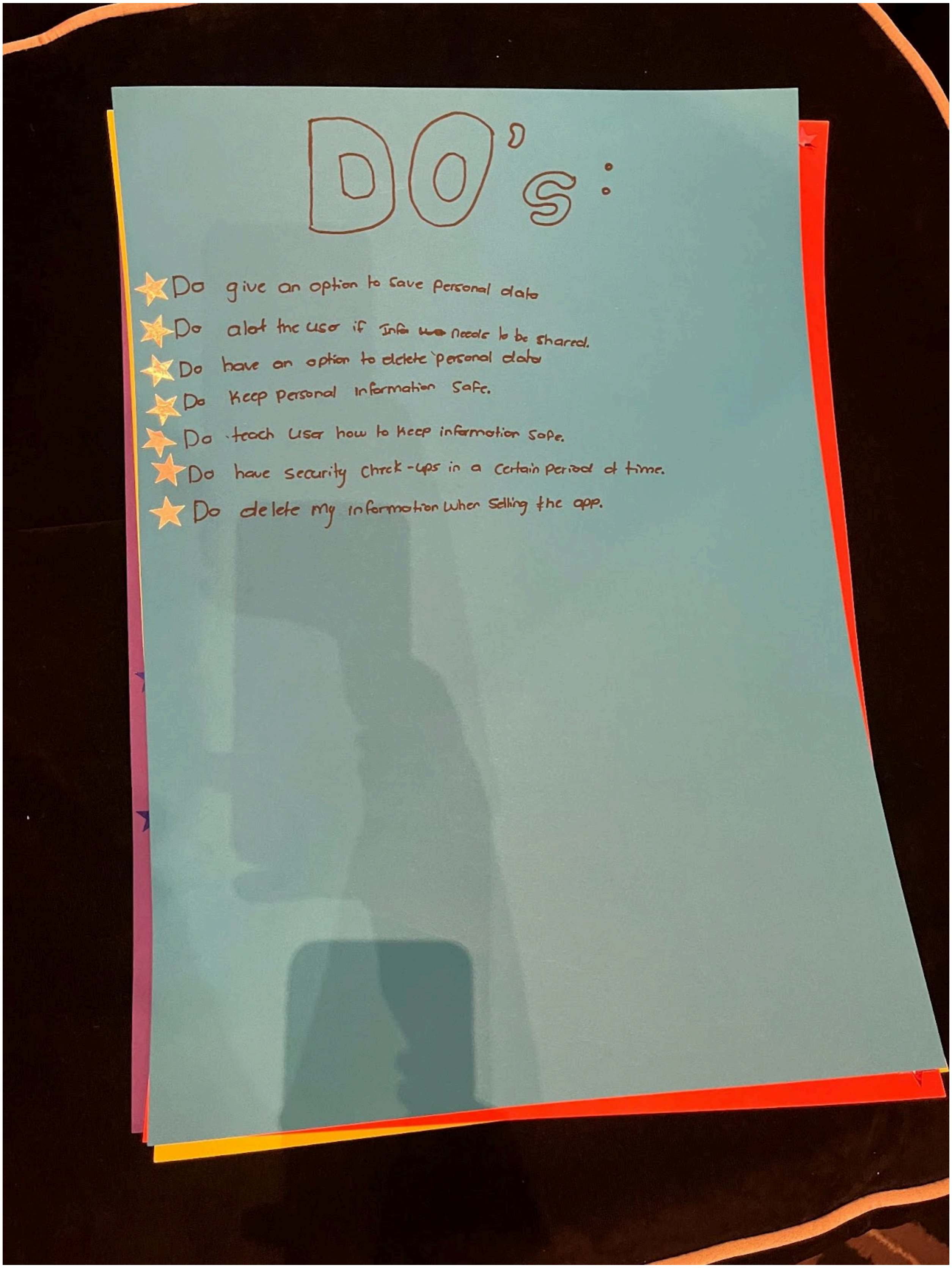
Doing monthly check ups with what they are doing with our data.

If a company is sold, the company should make sure ~~that~~ the company their to they should ~~w~~ used it for melicious intent

Information to be kept within that specific company (no third parties)

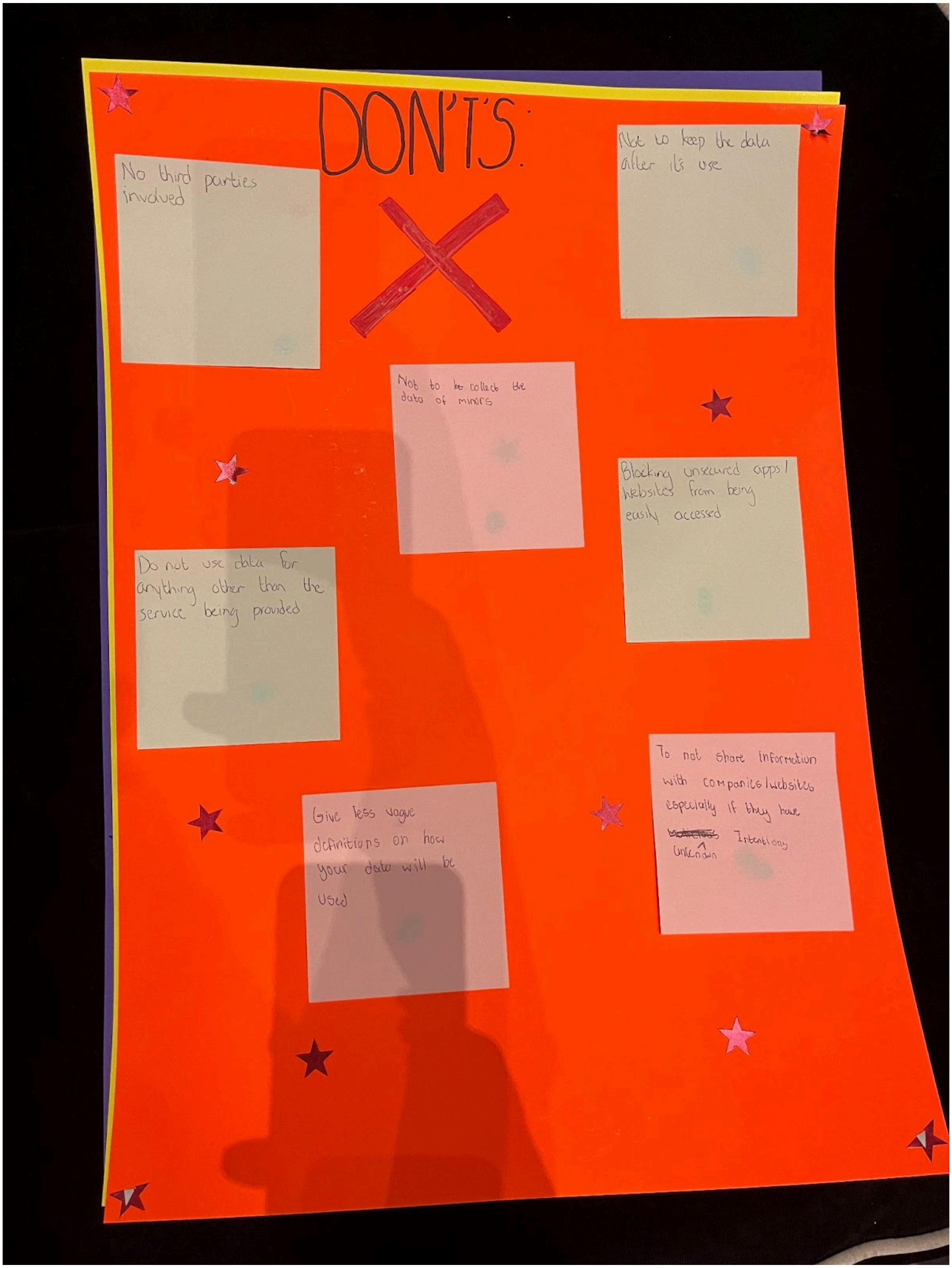
To ensure companies have strong firewall systems that won't allow hackers or perpatraitors to access personal data

~~Don't~~ = They should explain or eleborate more on the terms being used in the terms and policy contract These are terms which are mostly understood by the people of the company and they should explain the terms in depth



DO's:

- Do give an option to save personal data
- Do alart the user if Info needs to be shared.
- Do have an option to delete personal data
- Do keep personal information safe.
- Do teach user how to keep information safe.
- Do have security check-ups in a certain period of time.
- Do delete my information when selling the app.



DON'T'S:

No third parties involved

Not to keep the data after it's use

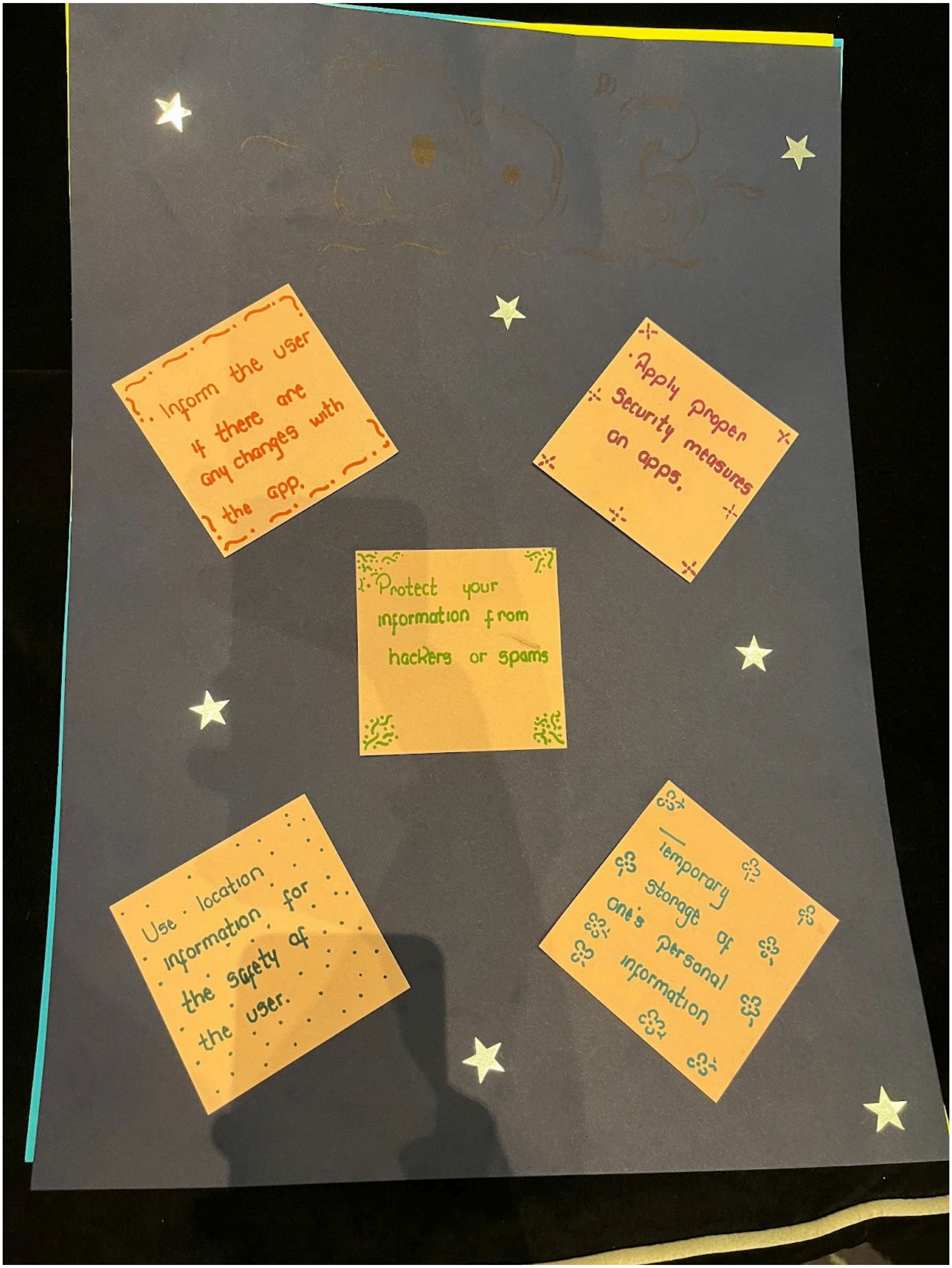
Not to ~~ke~~ collect the data of minors

Blocking unsecured apps / websites from being easily accessed

Do not use data for anything other than the service being provided

To not share information with companies/websites especially if they have ~~Malicious~~ Unknown Intentions

Give less vague definitions on how your data will be used



DO'S

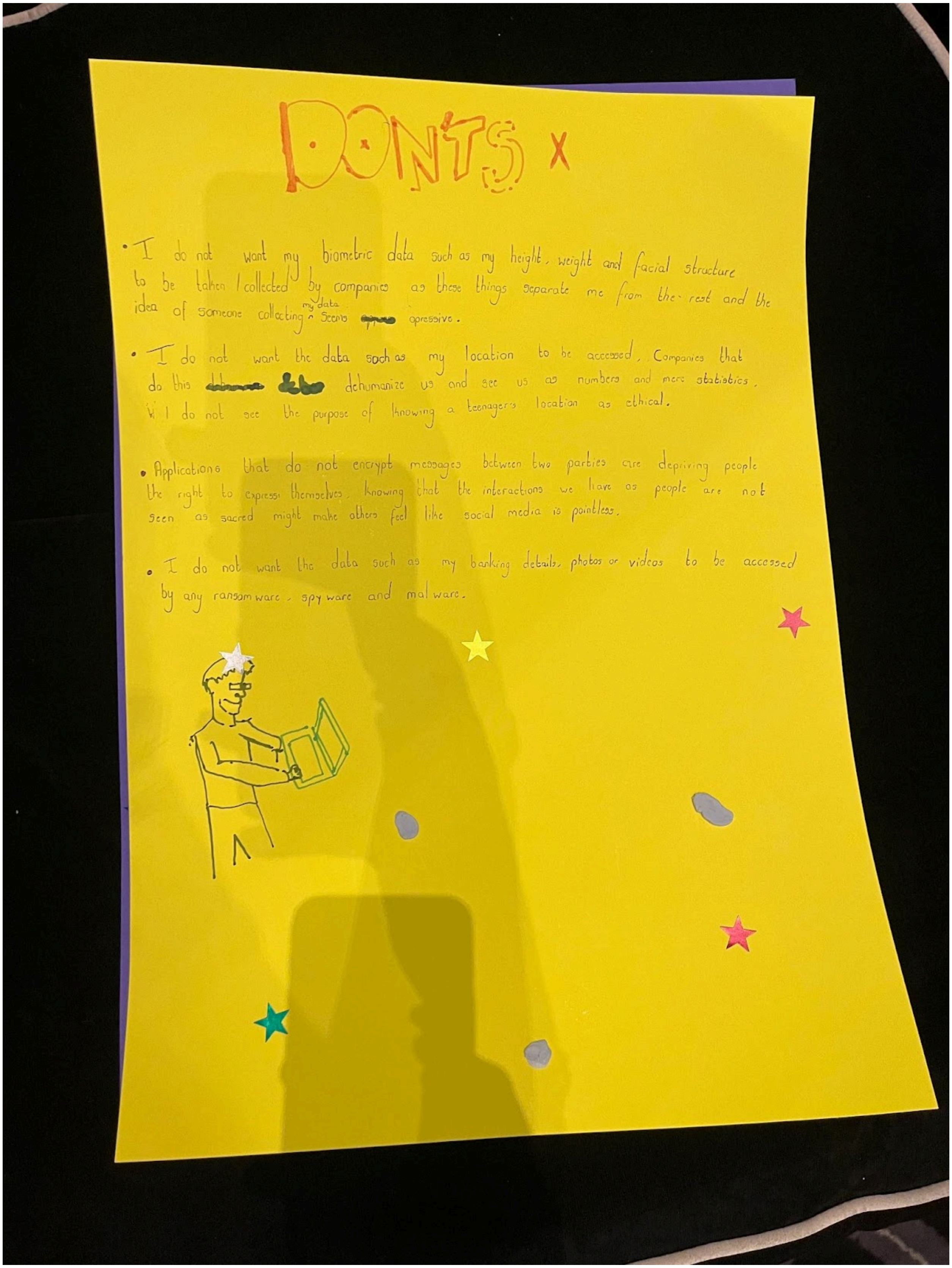
Inform the user if there are any changes with the app.

Apply proper Security measures on apps.

Protect your information from hackers or spams

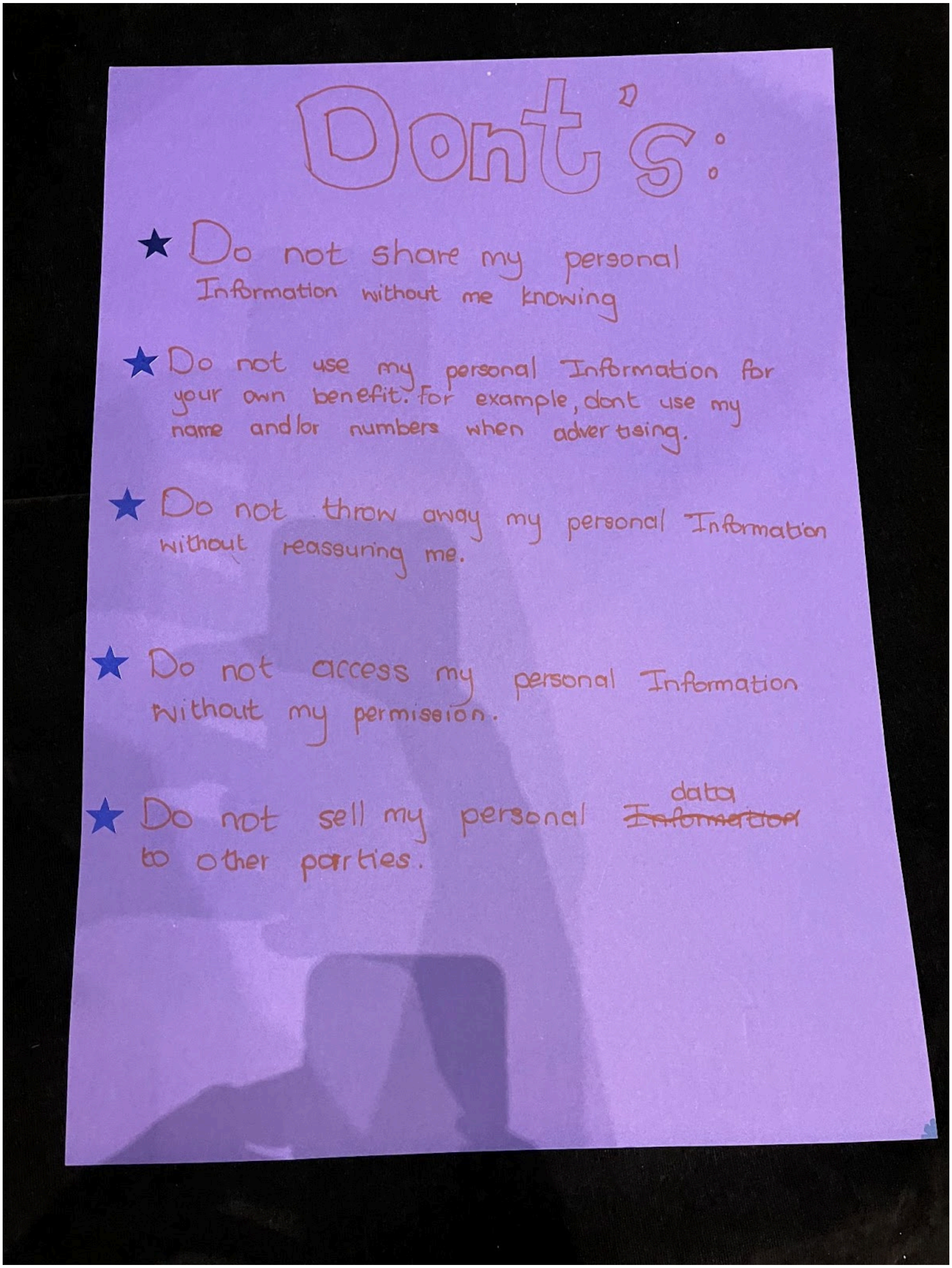
Use location information for the safety of the user.

Temporary Storage of One's Personal information



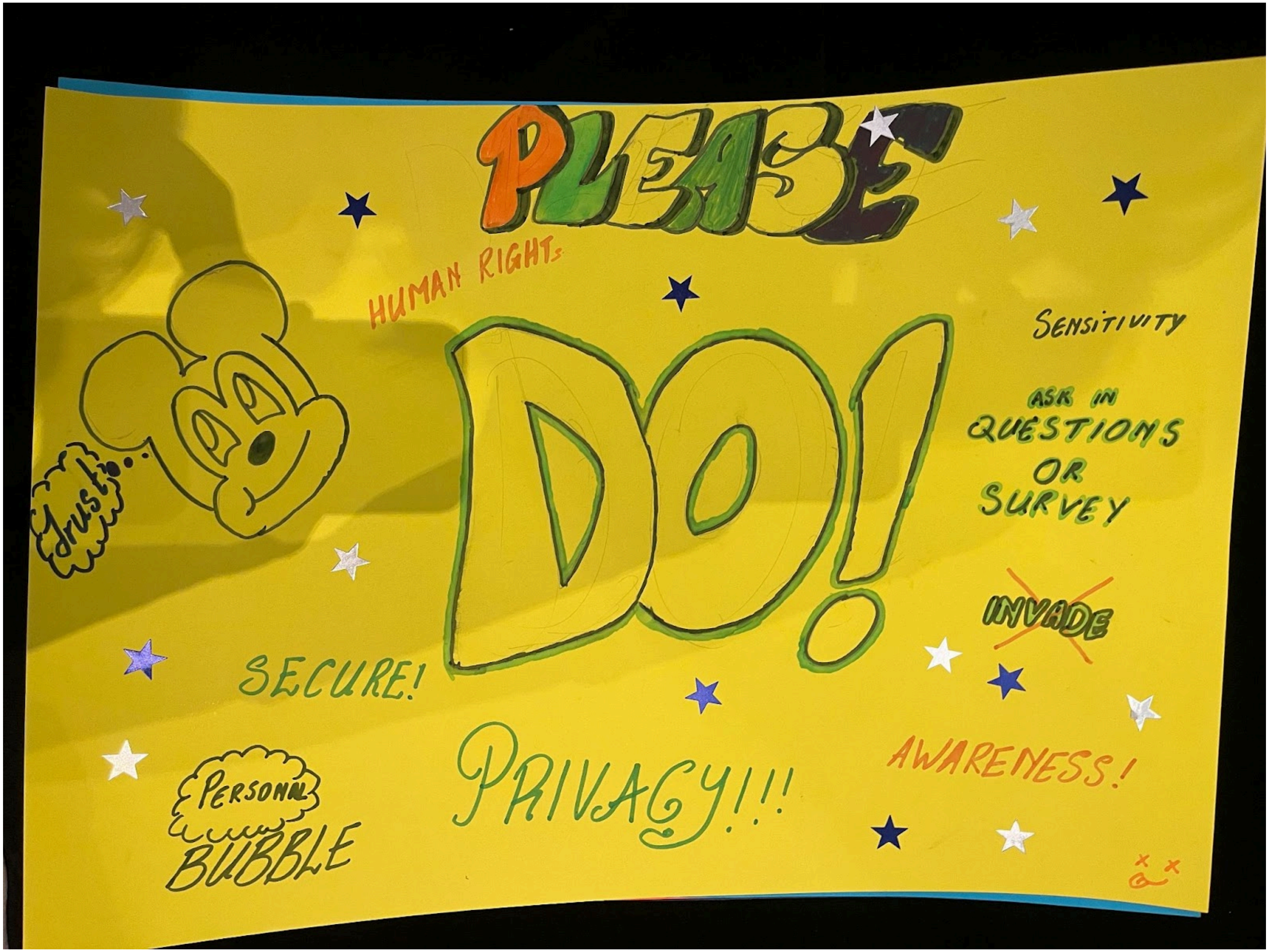
DONTS X

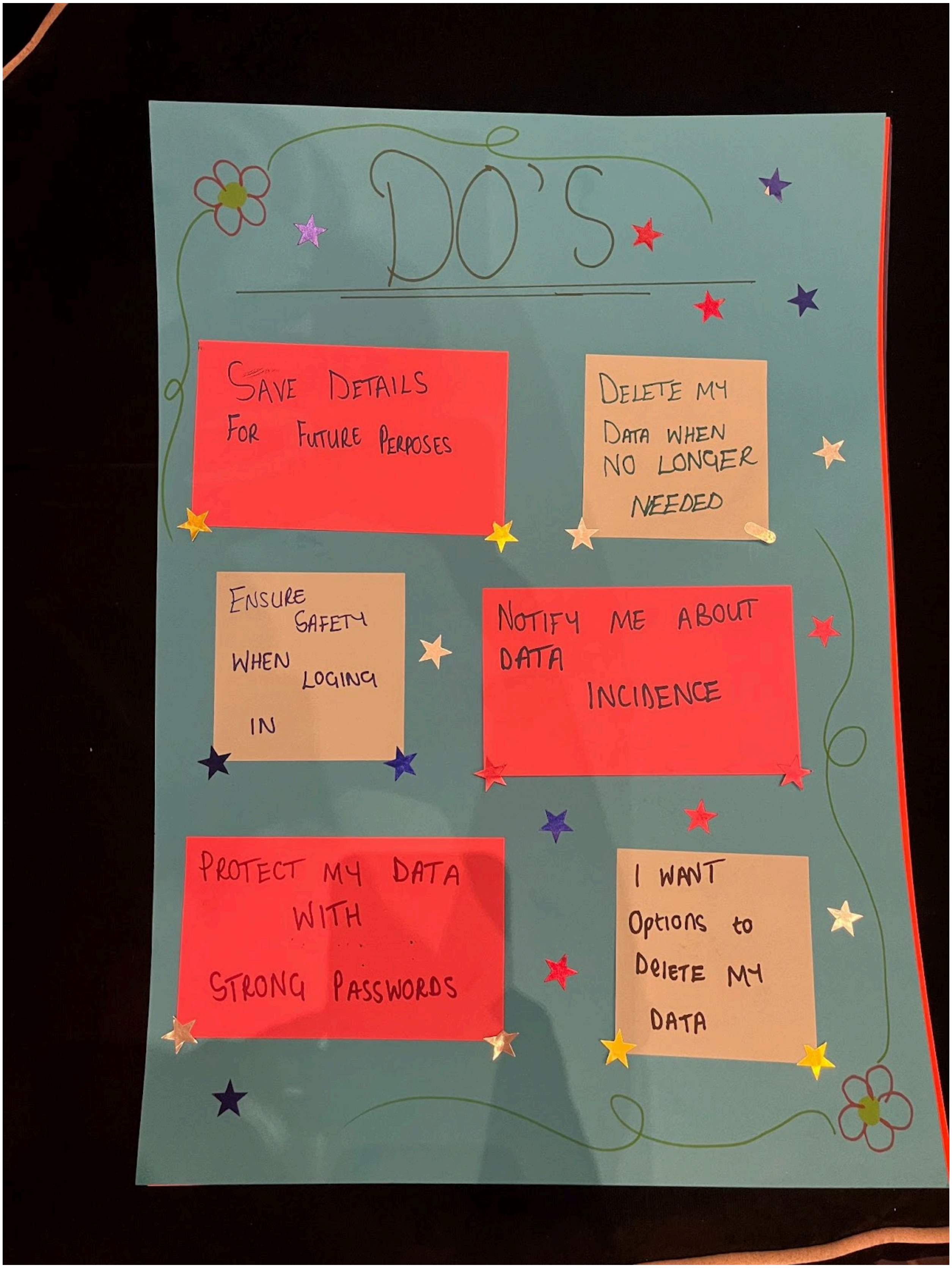
- I do not want my biometric data such as my height, weight and facial structure to be taken / collected by companies as these things separate me from the rest and the idea of someone collecting my data seems opressive.
- I do not want the data such as my location to be accessed. Companies that do this dehumanize us and see us as numbers and mere statistics. I do not see the purpose of knowing a teenager's location as ethical.
- Applications that do not encrypt messages between two parties are depriving people the right to expressi themselves. Knowing that the interactions we have as people are not seen as sacred might make others feel like social media is pointless.
- I do not want the data such as my banking details, photos or videos to be accessed by any ransomware, spy ware and mal ware.



Dont's:

- ★ Do not share my personal Information without me knowing
- ★ Do not use my personal Information for your own benefit. For example, dont use my name and/or numbers when advertising.
- ★ Do not throw away my personal Information without reassuring me.
- ★ Do not access my personal Information without my permission.
- ★ Do not sell my personal ~~Information~~ data to other parties.


PLEASE
HUMAN RIGHTS
DO!
SENSITIVITY
ASK IN QUESTIONS OR SURVEY
~~INVADE~~
Trust!...
SECURE!
PRIVACY!!!
AWARENESS!
PERSONAL BUBBLE



DO'S

SAVE DETAILS FOR FUTURE PERPOSES

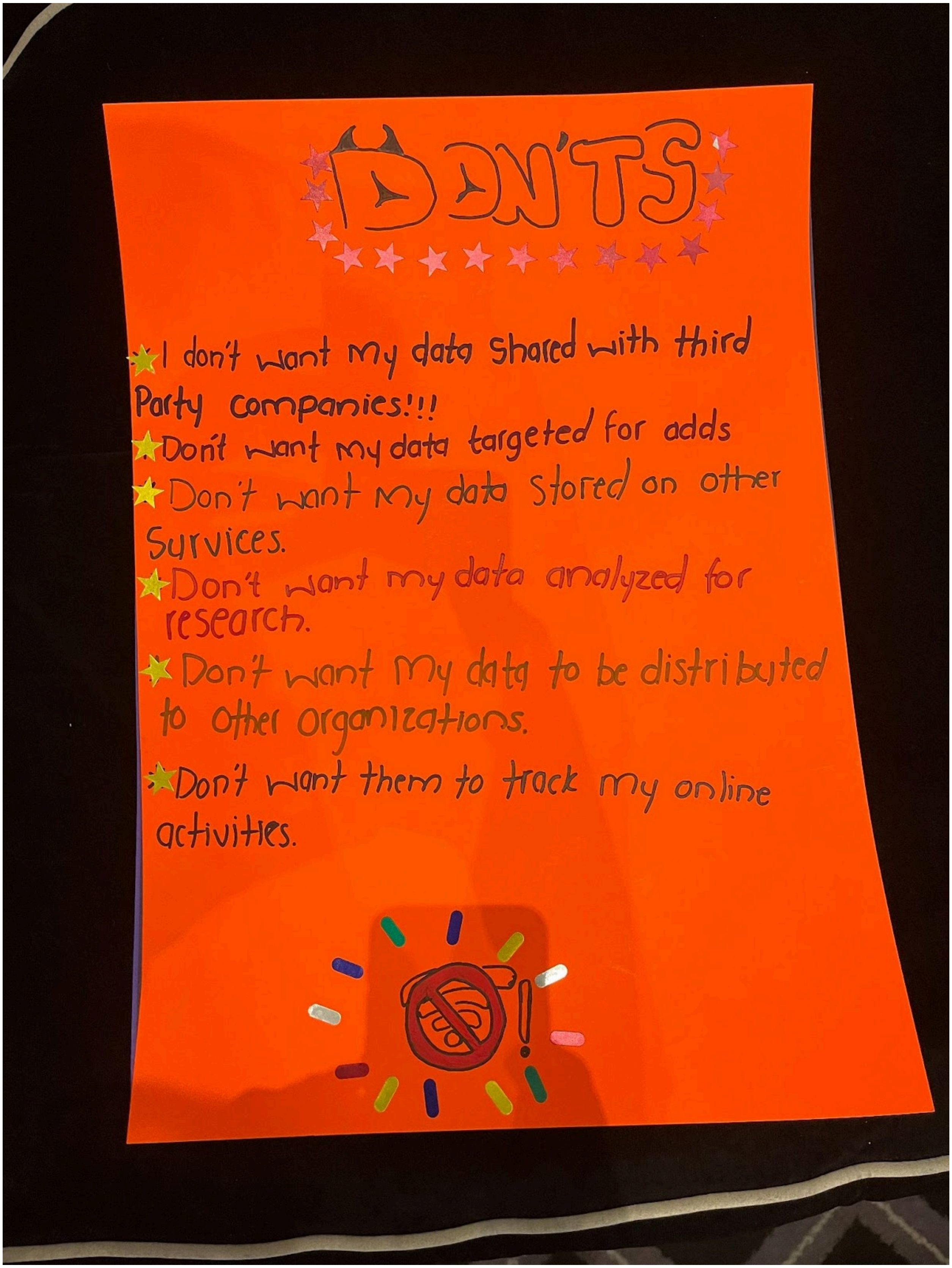
DELETE MY DATA WHEN NO LONGER NEEDED

ENSURE SAFETY WHEN LOGING IN

NOTIFY ME ABOUT DATA INCIDENCE

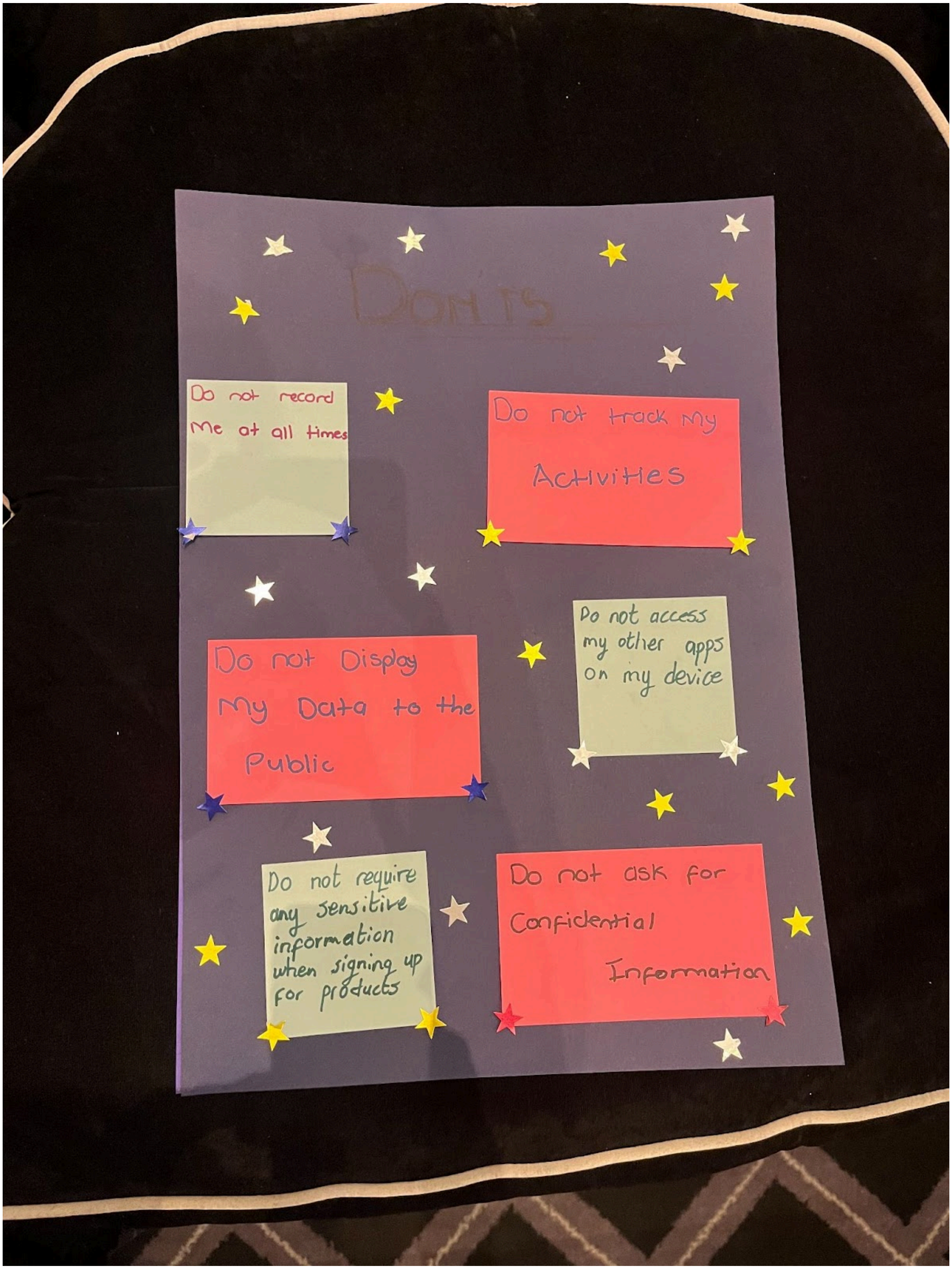
PROTECT MY DATA WITH STRONG PASSWORDS

I WANT Options to DeleTE MY DATA



DON'TS

- I don't want my data shared with third Party companies!!!
- Don't want my data targeted for adds
- Don't want my data stored on other Survices.
- Don't want my data analyzed for research.
- Don't want my data to be distributed to other organizations.
- Don't want them to track my online activities.



DON'TS

Do not record
Me at all times

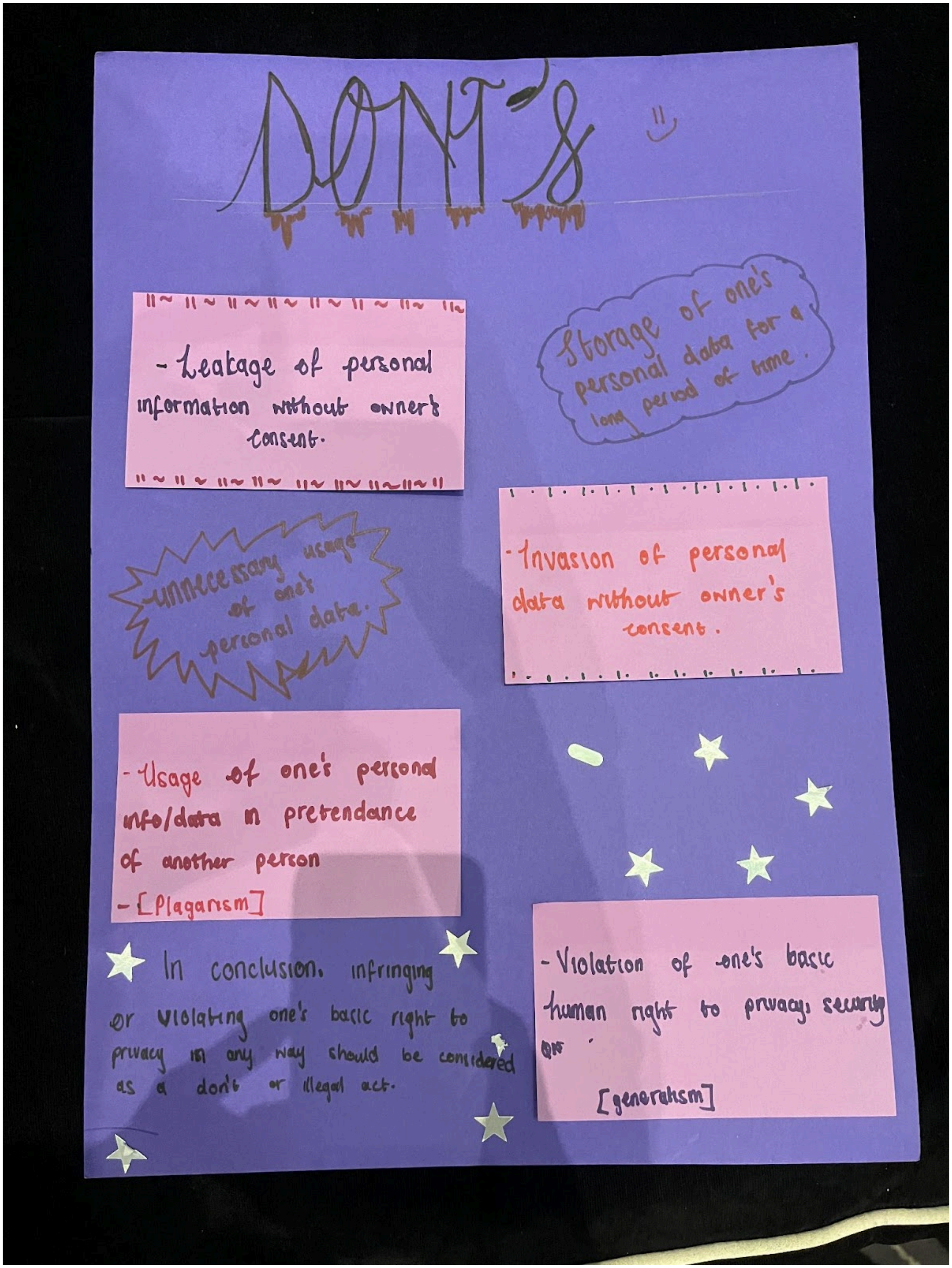
Do not track My
Activities

Do not Display
My Data to the
Public

Do not access
my other apps
on my device

Do not require
any sensitive
information
when signing up
for products

Do not ask for
Confidential
Information



DONT'S

- Leakage of personal information without owner's consent.

Storage of one's personal data for a long period of time.

- unnecessary usage of one's personal data.

- Invasion of personal data without owner's consent.

- Usage of one's personal info/data in pretendance of another person

- [Plagarism]

In conclusion, infringing or violating one's basic right to privacy in any way should be considered as a don't or illegal act.

- Violation of one's basic human right to privacy, security or .

[generalism]