

NEXT GENERATION AI RESEARCH CENTRE



We Stand Against Cyberbullying



Cybersecurity and Online Safety Analysis

Student Cyberbullying Awareness Survey: Findings and Concerning Issues

Prepared from a cybersecurity and online safety advisory perspective
Analysis phase document: issues identified only, no recommendations included



16 July 2026



Data source: student_cyberbullying_survey_sample.csv
(n = 512, fully anonymous, no identifying information collected)



Prepared By

Dr Abdullahi Chowdhury, SMIEEE

Research Director (Collaboration & Partnership)
Next Generation AI Research Centre



<https://ngairc.com/awareness.html>

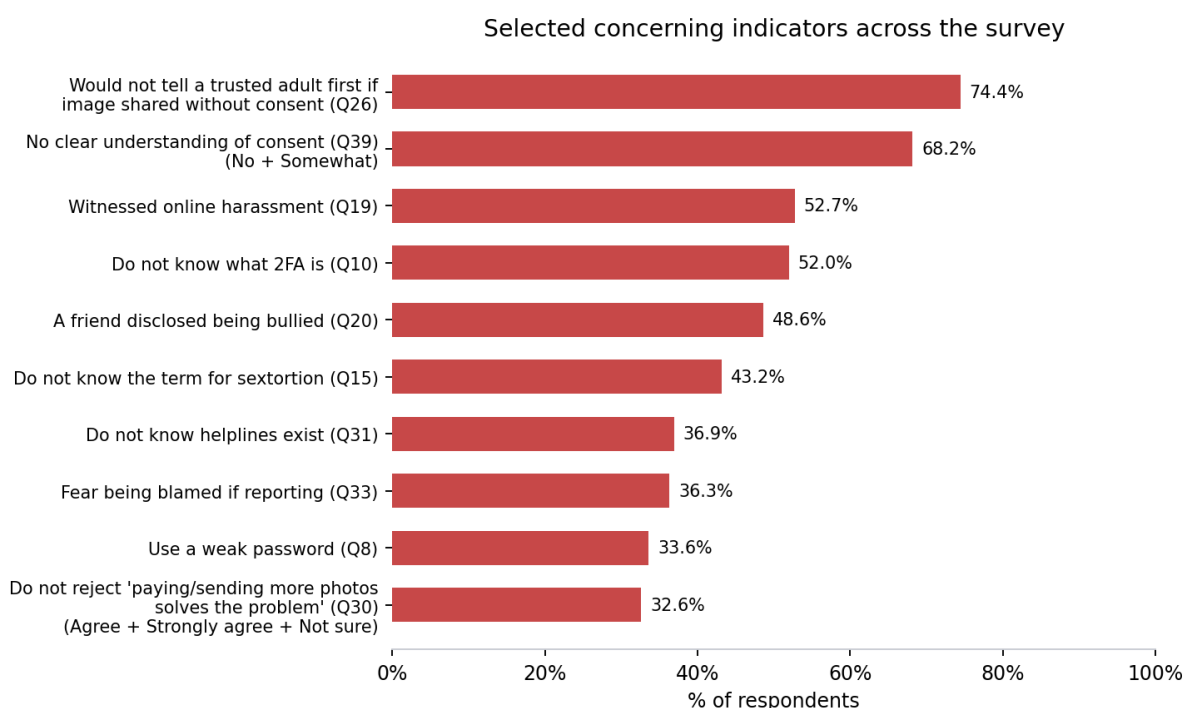
Executive Summary

Overview of purpose, scope and headline findings

This report presents a cybersecurity and online safety analysis of an anonymous awareness survey completed by 512 students (mean age 15.1 years, range 13–17) as part of the Next Generation AI Research Centre (NGAIRC) cyberbullying prevention initiative. The survey instrument covered six domains: basic demographic information, internet use and account security practices, conceptual understanding of cyberbullying and online harassment, direct experience and observation of online harm, awareness of rights and support pathways, and personal responsibility and online behaviour.

The analysis identifies a consistent pattern across the dataset. A majority of respondents hold broadly appropriate attitudes toward online safety and the wrongness of harassment (for example, 80.1% agree that posting someone's content without consent is wrong, and 74.0% reject victim-blaming). However, there are substantial, and in several cases severe, gaps between stated attitude and operational knowledge, particularly in account security hygiene, incident response knowledge, and awareness of support pathways. These gaps sit alongside a high self-reported prevalence of exposure to online harm: 52.7% of respondents have witnessed online harassment directly, and 48.6% have had a friend disclose being bullied or threatened online.

The chart below summarises ten of the more concerning indicators surfaced across the survey. Each is discussed in the relevant section of this report, with reference to its implications from a cybersecurity and child online safety perspective.



Overview 1. Selected concerning indicators across the survey (n = 512).

Consistent with the scope agreed for this phase of work, this report documents concerning issues only. It does not propose remedial actions, interventions or recommendations. The next step is for NGAIRC advisors to monitor, further analyse and interpret these findings, and to determine and provide an appropriate programme update.

Methodology Note

Survey design and interpretive limitations

The survey was administered as a fully anonymous, self-report questionnaire; no names or identifying information were collected. It comprised 40 items across six sections (A–F), using single-choice, multiple-choice and five-point agreement scale formats. Responses were collected across three school groupings; school-level comparison is outside the scope of this report, which analyses the 512 responses as a single cohort.

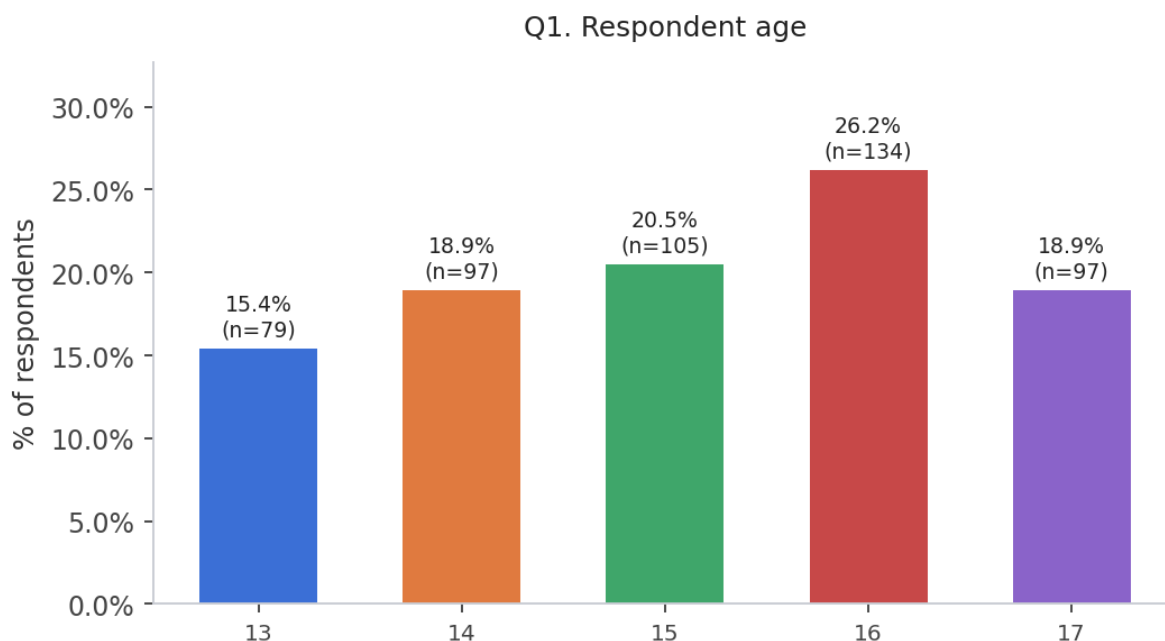
As with all self-report data, findings reflect stated perceptions, knowledge and intended or recalled behaviour rather than independently verified or observed behaviour and are subject to social desirability bias. This is particularly relevant to sensitive items such as question 35 (sharing someone else's content without permission), where under-reporting is likely. Percentages throughout this report are calculated against the number of respondents who answered the relevant item; multiple-choice items (questions 3 and 12) permit more than one selection, so their percentages do not sum to 100%.

Charts are presented for every one of the 40 survey questions, organised by section, together with four summary charts that consolidate related indicators for ease of reference.

A. Basic Information

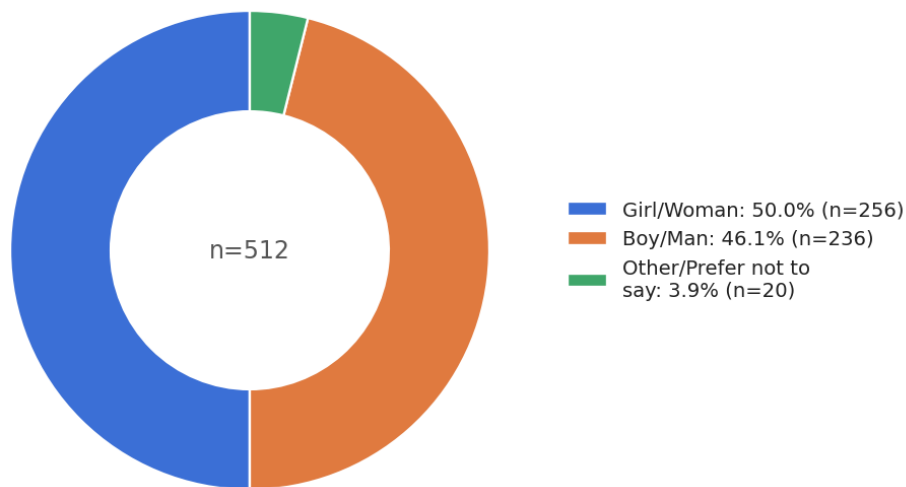
Respondent demographic profile

The sample is broadly evenly distributed across the 13–17 age range (13: 15.4%, 14: 18.9%, 15: 20.5%, 16: 26.2%, 17: 18.9%) and by gender (50.0% girl/woman, 46.1% boy/man, 3.9% other/prefer not to say). This demographic profile is directly relevant to the interpretation of every subsequent finding: the entire cohort is a minor population, for whom the threshold of concern regarding account compromise, unsolicited contact, online exploitation and image-based abuse is inherently lower than it would be for an adult population, and for whom protective statutory and platform frameworks (age of digital consent, child safety reporting obligations) are typically engaged.



Q1. Respondent age (n = 512).

Q2. Respondent gender



Q2. Respondent gender (n = 512).

B Internet Use & Account Security Hygiene

How students connect, and how securely

This section carries the most direct cybersecurity relevance of the survey. Time spent online is substantial: 48.8% of respondents report 3 or more hours online per day. Before initiating contact with a new person online, only 47.9% report actively trying to verify who the person is; 40.6% chat without checking, and 11.5% are unsure. Taken together, just over half the cohort (52.1%) lacks a consistent contact-verification practice, a primary vector for grooming, catfishing and social engineering directed at minors.

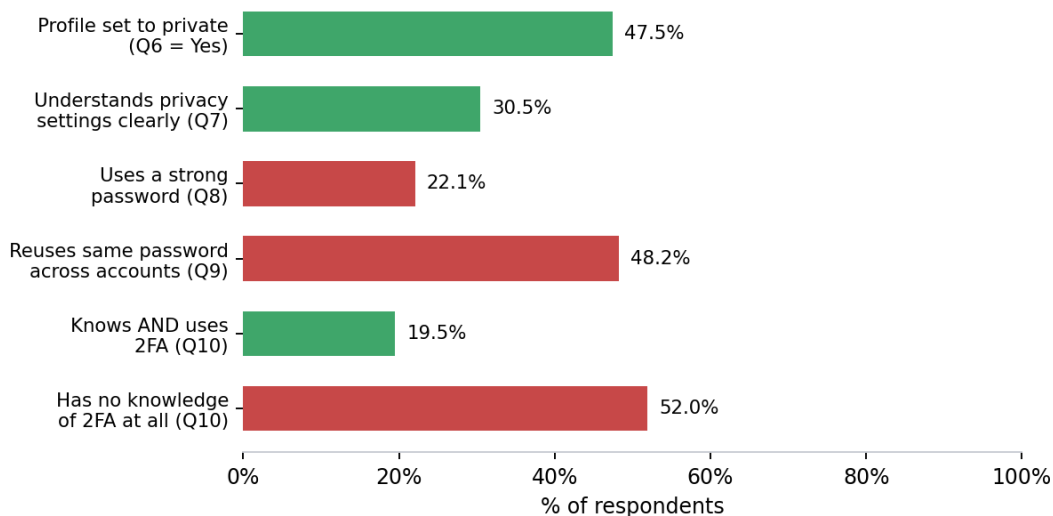
Profile configuration compounds this exposure. Only 47.5% report a private or restricted profile; 38.1% report a public profile and 14.5% are unsure of their own setting. Understanding of privacy settings is similarly limited: only 30.5% report understanding them clearly, 21.7% report no understanding at all, and 13.5% are unsure. A public or unconfigured profile, combined with a limited understanding of the controls governing it, creates a materially larger surface area for unsolicited contact and content harvesting.

Credential hygiene is a significant weak point. Only 22.1% of respondents report using a strong password; 33.6% report a weak password (a name, birthday, or a simple numeric sequence), and 33.2% report a medium-strength password. This is compounded by password reuse: 48.2% reuse the same password across multiple apps or accounts. The co-occurrence of weak and reused passwords is significant because it materially increases the likelihood that the compromise of a single low-value account (for example, a game or forum login) cascades into the compromise of higher-value accounts, such as social media or email, a classic credential-stuffing risk pathway.

The weakest control identified anywhere in the survey is multi-factor authentication. 52.0% of respondents do not know what two-factor authentication (2FA) is, and only 19.5% both know of it and actively use it. Combined with the password findings above, this indicates that account takeover, itself frequently a precursor to impersonation, further harassment or image-based abuse, is a structurally under-mitigated risk across this population.

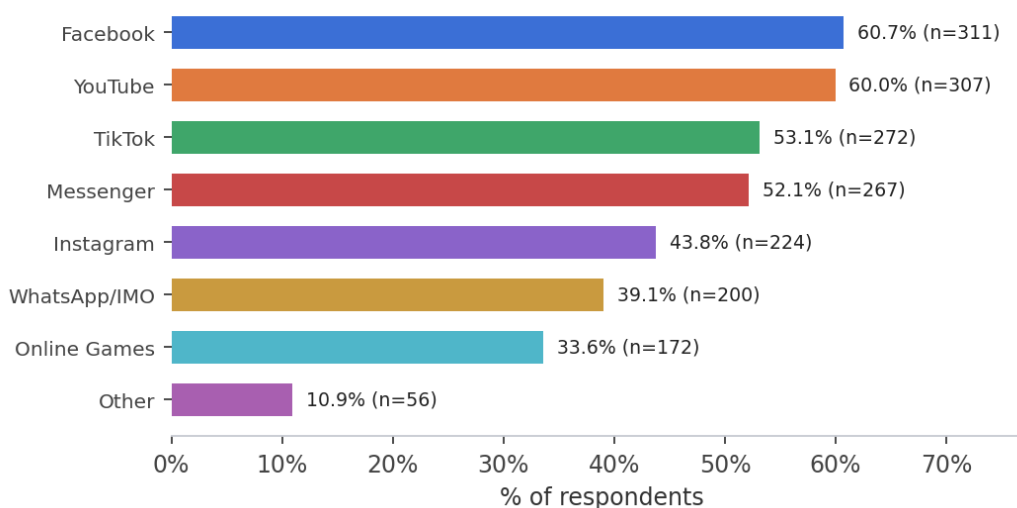
NEXT GENERATION AI RESEARCH CENTRE

Account security hygiene snapshot



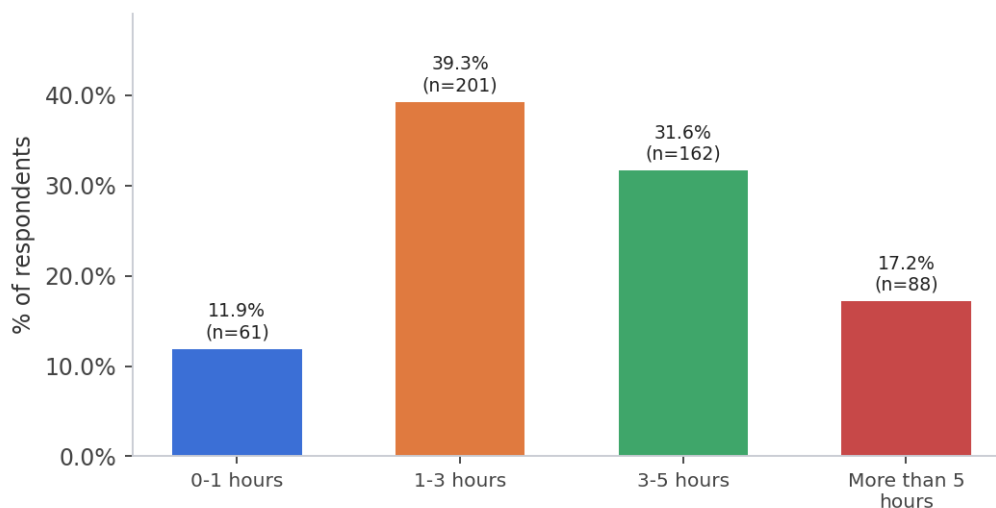
Overview 2. Account security hygiene snapshot (n = 512).

Q3. Platforms used most (multiple answers allowed)



Q3. Platforms used most, multiple answers allowed (n = 512 respondents).

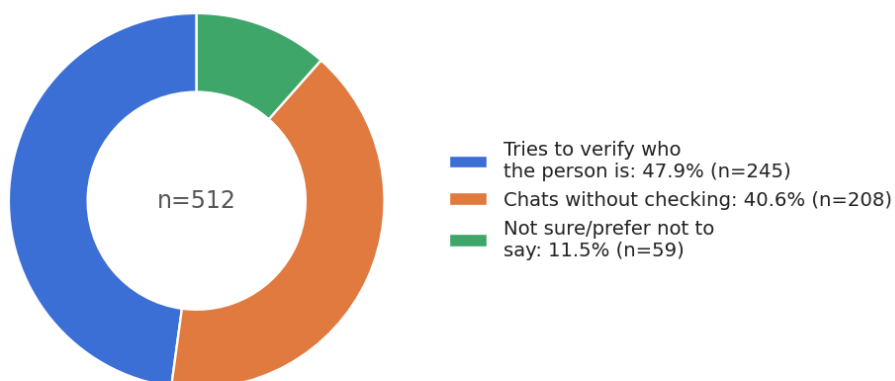
Q4. Average daily time spent online



Q4. Average daily time spent online (n = 512).

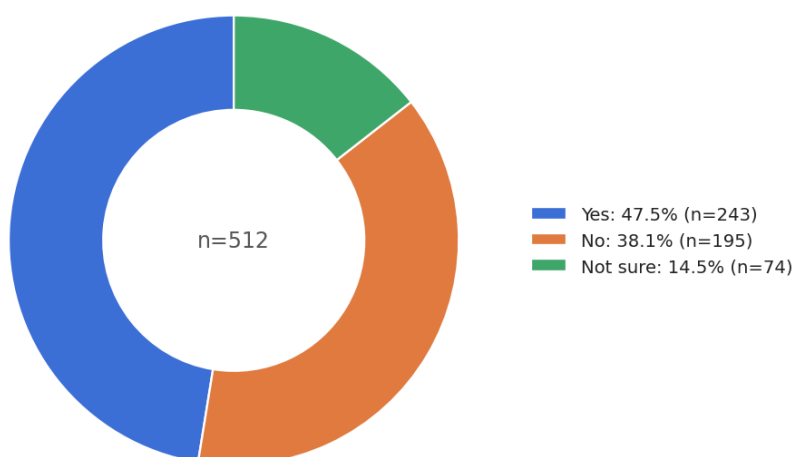
NEXT GENERATION AI RESEARCH CENTRE

Q5. Action before chatting with a new online contact



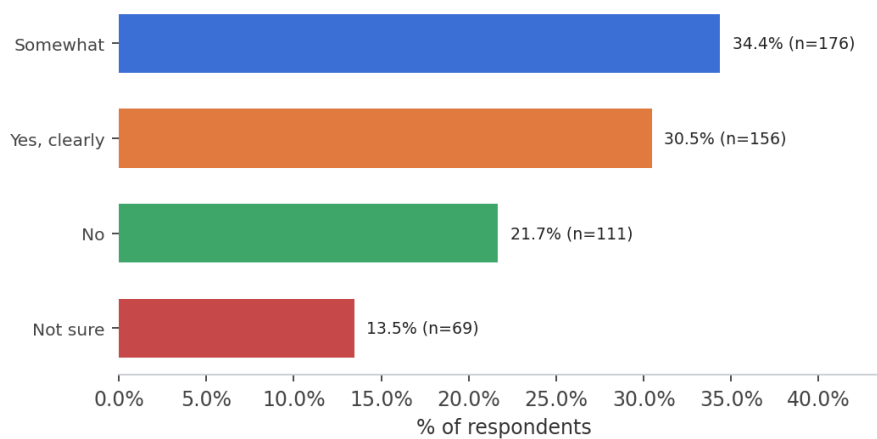
Q5. Action before chatting with a new online contact (n = 512).

Q6. Social media profile set to private



Q6. Social media profile set to private (n = 512).

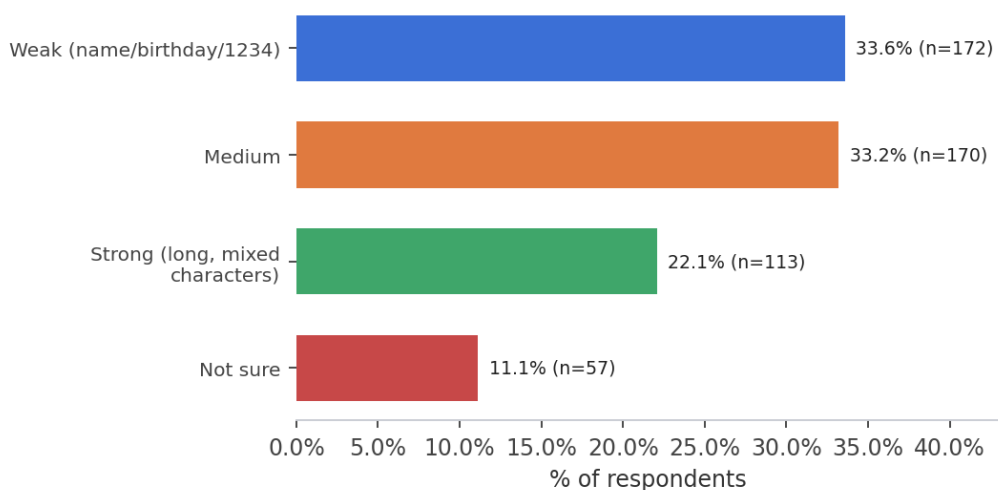
Q7. Understands what privacy settings are and why they matter



Q7. Understanding of privacy settings and their importance (n = 512).

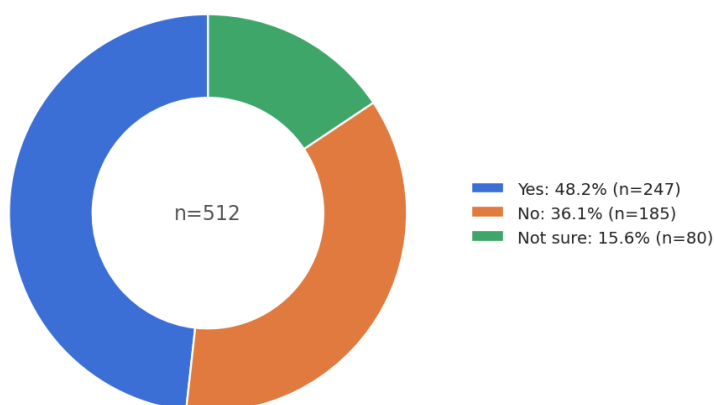
NEXT GENERATION AI RESEARCH CENTRE

Q8. Password strength type



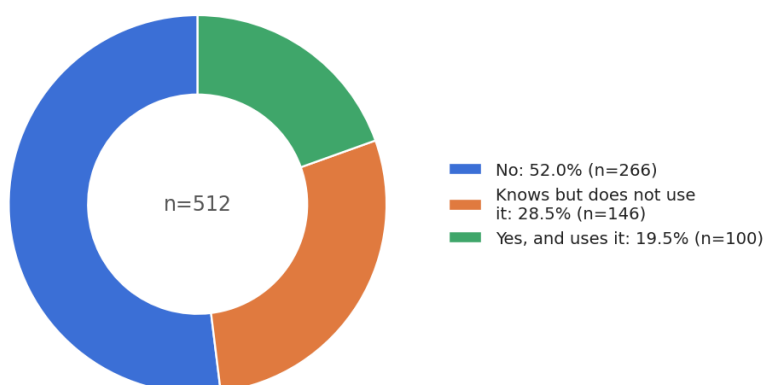
Q8. Password strength type (n = 512).

Q9. Reuses the same password across accounts/apps



Q9. Reuses the same password across accounts/apps (n = 512).

Q10. Knowledge and use of two-factor authentication (2FA)



Q10. Knowledge and use of two-factor authentication (n = 512).

C. Understanding of Cyberbullying

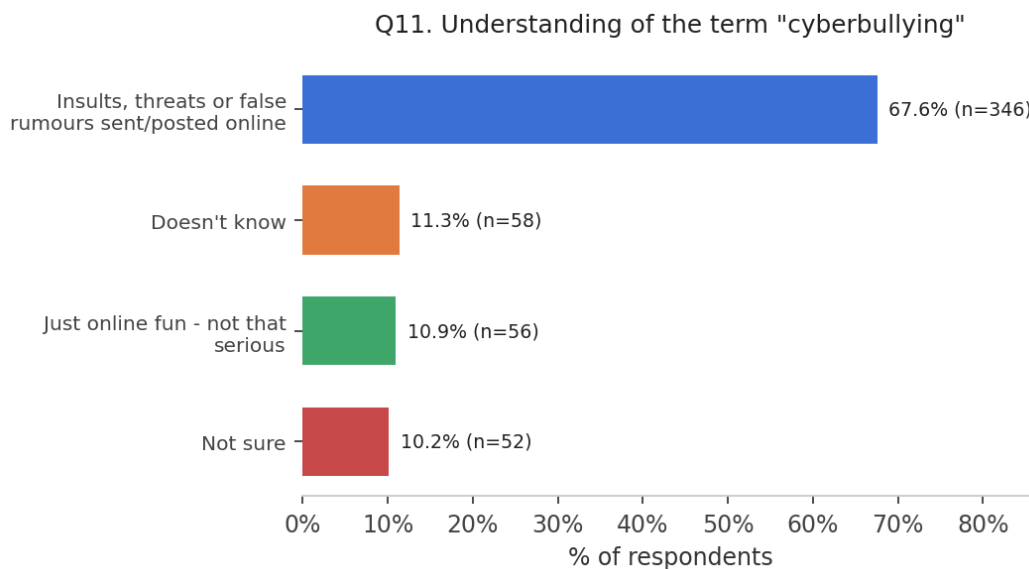
What students know about online harm

Definitional understanding of cyberbullying is reasonably strong: 67.6% of respondents correctly characterise it as insults, threats or false rumours sent or posted online. However, 22.2% either do not know the definition or classify it as "just online fun, not that serious", a minimisation framing that recurs at several points later in the survey.

Whether trolling and harassment are the same thing produced a near three-way split (40.2% no, 39.1% yes, 20.7% not sure). This indicates the cohort holds no shared, consistent understanding of where informal online provocation ends and harassment begins, which is relevant because it affects a respondent's threshold for recognising when their own conduct, or a peer's, has crossed into harassment.

One of the more concerning findings in this section concerns sextortion literacy. Only 30.3% of respondents know the specific term for online sextortion (being threatened for money, photos or favours); 43.2% do not, and 26.6% are unsure. Online sextortion targeting minors is a well-documented and escalating harm category internationally, and this result indicates a substantial vocabulary and recognition gap within a population that sits directly inside the age range most frequently targeted by this crime type.

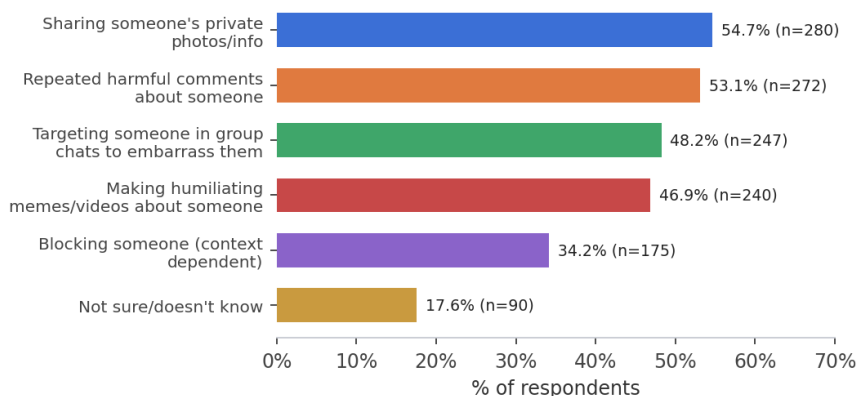
Awareness of AI-generated fake imagery is similarly limited: only 38.3% report clear awareness that AI can create fake images or video, 34.4% have "heard a little", and 27.3% report no awareness at all. Because the survey subsequently tests recognition of AI-generated fake imagery as a form of abuse (question 18), this gap indicates that a meaningful minority of respondents may lack the technical vocabulary to identify or describe this harm if they encountered it. On the related question of whether such fabricated imagery constitutes abuse, 80.1% answered correctly, though 19.9% remained unsure or disagreed, despite a comparatively unambiguous correct answer.



Q11. Understanding of the term "cyberbullying" (n = 512).

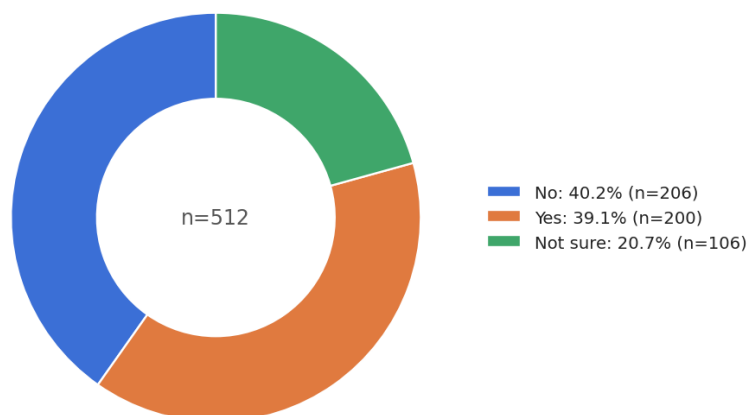
NEXT GENERATION AI RESEARCH CENTRE

Q12. Behaviours recognised as cyberbullying / online harassment (multiple answers allowed)



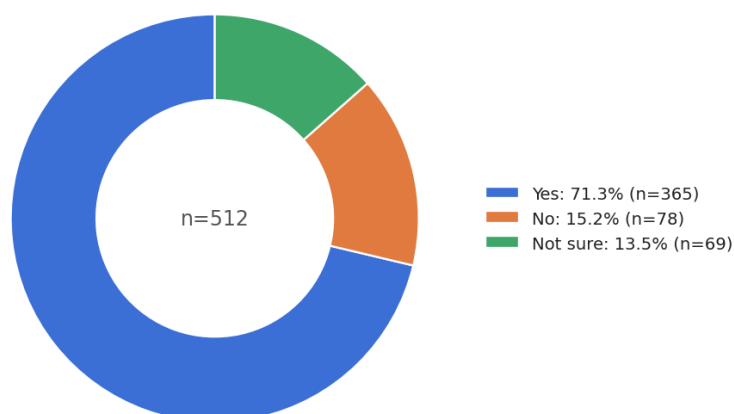
Q12. Behaviours recognised as cyberbullying, multiple answers allowed (n = 512 respondents).

Q13. Belief that trolling and harassment are the same thing



Q13. Belief that trolling and harassment are the same thing (n = 512).

Q14. Repeated unwanted messaging recognised as harassment

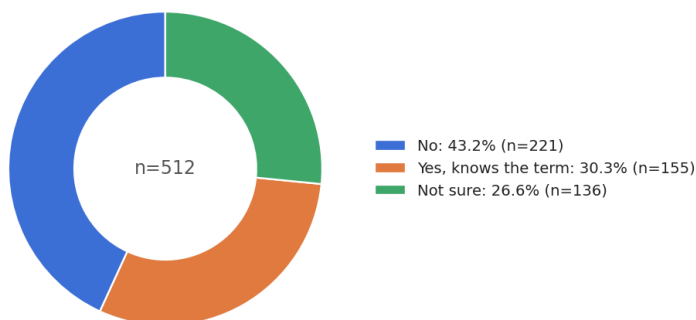


Q14. Repeated
recognised as

unwanted messaging
harassment (n = 512).

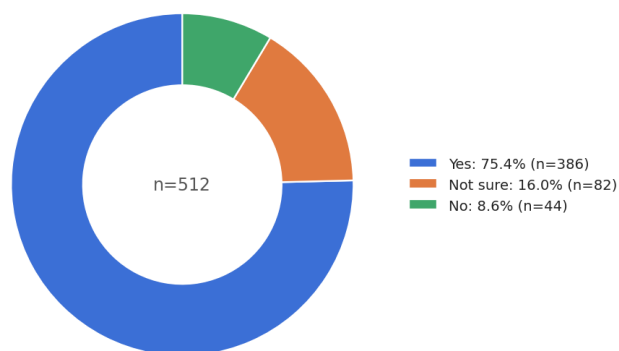
NEXT GENERATION AI RESEARCH CENTRE

Q15. Awareness of the term for online sextortion



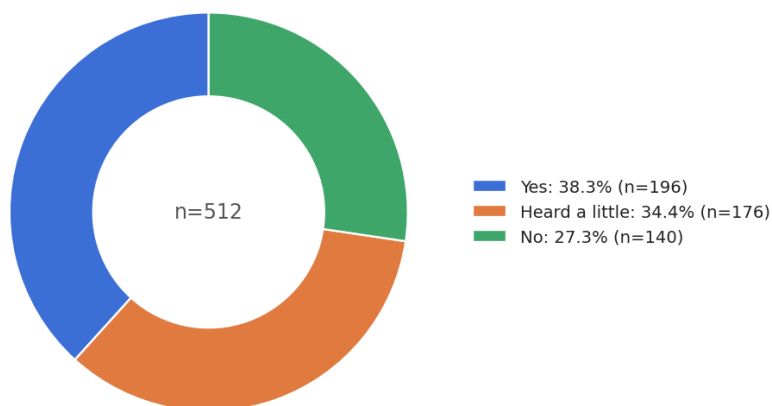
Q15. Awareness of the term for online sextortion (n = 512).

Q16. Belief that fake accounts/identities can cause real harm



Q16. Belief that fake accounts/identities can cause real harm (n = 512).

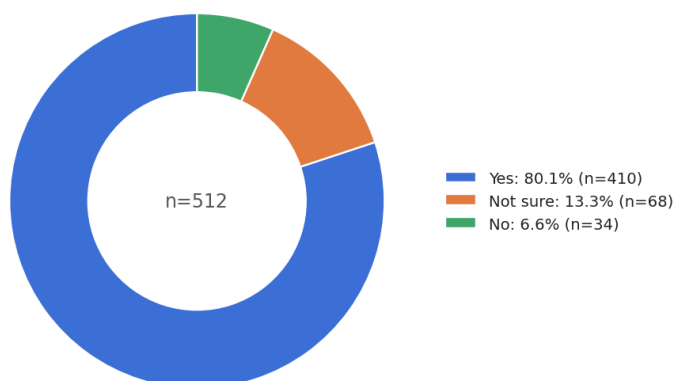
Q17. Awareness that AI can create fake images/video (deepfakes)



Q17. Awareness that AI can create fake images/video, i.e. deepfakes (n = 512).

NEXT GENERATION AI RESEARCH CENTRE

Q18. Recognises AI-generated fake sexual images/video as abuse



Q18. Recognition of AI-generated fake imagery as abuse (n = 512).

D. Experience & Observation

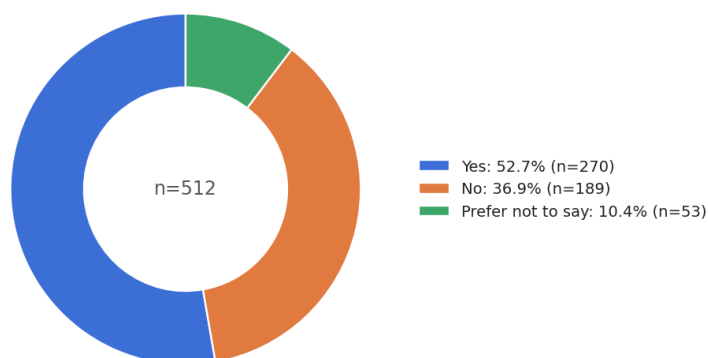
What students have witnessed or been told

Direct and secondhand exposure to online harassment is a near-majority experience within this cohort, rather than an isolated one. 52.7% of respondents have personally witnessed someone being harassed or bullied online, and 48.6% have had a friend disclose that they were bullied or threatened online.

Against this prevalence, the perceived importance of the issue shows a notable gap. While 69.4% agree or strongly agree that online harassment at their school or in their community is an important problem, 30.6% are either unsure (17.8%) or disagree (12.9% combined). Given the prevalence figures above, this gap suggests a degree of under-recognition of the problem's significance relative to its reported occurrence.

Consensus on gendered risk is comparatively low: only 52.8% (30.9% agree, 21.9% strongly agree) affirm that girls are more at risk online than boys, with 30.1% unsure. This is a lower level of agreement than the broader evidence base on gender differences in online risk might suggest and may indicate a gap in awareness of this pattern. Similarly, while 69.8% agree that online "fun" can seriously harm others, 14.5% disagree, and 15.8% are unsure, indicating a "just a joke" framing persists among a meaningful minority, a framing frequently present in bystander and perpetrator rationalisations of harassment.

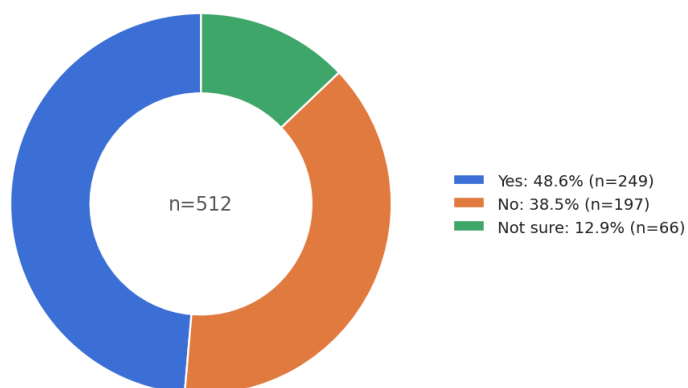
Q19. Has personally witnessed someone being harassed/bullied online



Q19. Has personally witnessed someone being harassed/bullied online (n = 512).

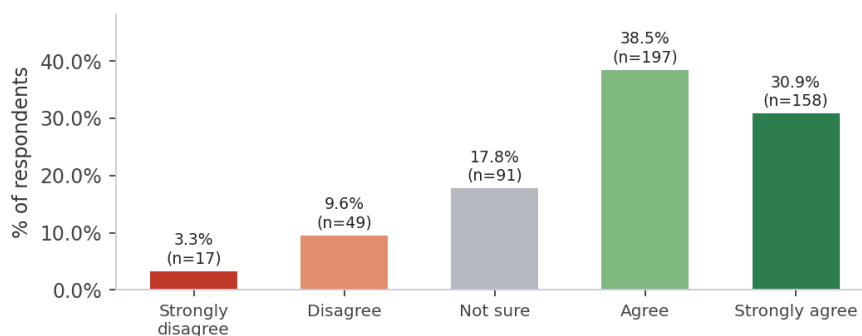
NEXT GENERATION AI RESEARCH CENTRE

Q20. A friend has disclosed being bullied/threatened online



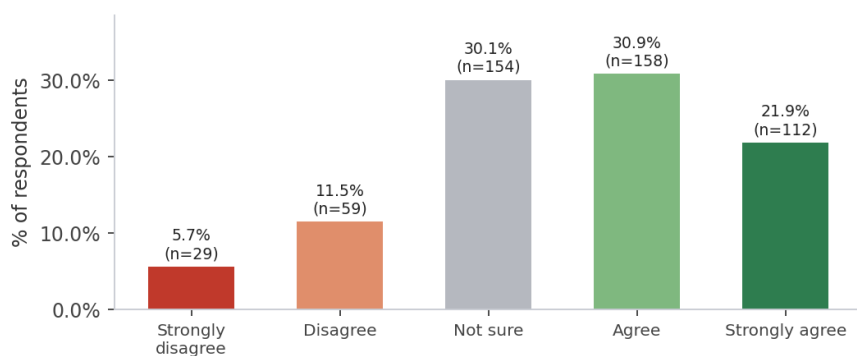
Q20. A friend has disclosed being bullied/threatened online (n = 512).

Q21. "Online harassment at my school/community is an important problem"



Q21. "Online harassment at my school/community is an important problem" (n = 512).

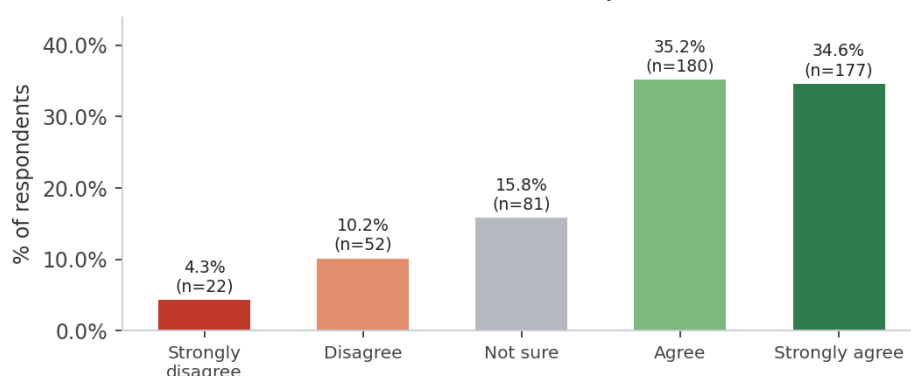
Q22. "Girls are more at risk online than boys"



Q22. "Girls are more at risk online than boys" (n = 512).

NEXT GENERATION AI RESEARCH CENTRE

Q23. "Online 'fun' can seriously harm others"



Q23. "Online 'fun' can seriously harm others" (n = 512).

E. Rights, Safety & Getting Support

Awareness of rights and support pathways

This is the section with the most significant implications for incident response and victim support. A strong majority (81.7%) affirm the basic right to be safe online, while 18.3% remain neutral or disagree with this statement. When asked what they would do first if a photo or video were shared without their consent, only 25.6% selected "tell a trusted adult"; 27.0% would block or report the person themselves, 26.0% would ask the perpetrator directly to delete it (a response that involves direct re-engagement with a potential offender), and 9.4% would stay silent and hope it resolves itself. The low rate of adult disclosure as a first response, combined with the near one-in-ten who would take no action, indicates a support-seeking gap in precisely the harm category, image-based abuse, that carries the highest risk of escalation if handled without adult or institutional support.

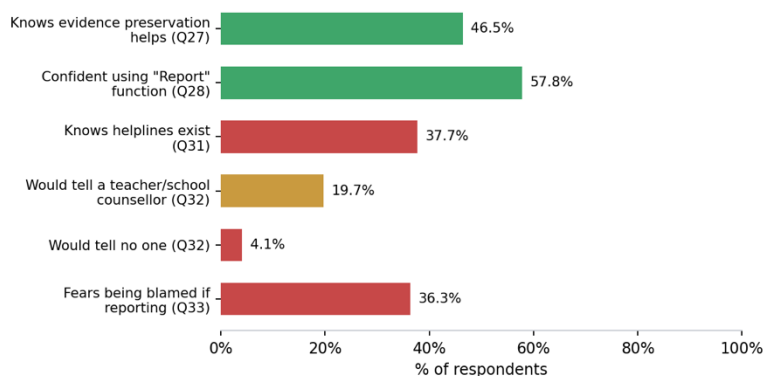
Foundational incident-response knowledge is limited. Only 46.5% know that preserving screenshots, links, and timestamps helps respond to online harassment; the remaining 53.5% either do not know this or are unsure. Confidence in using platform safety tools is similarly incomplete: only 57.8% are confident they could locate and use the "Report" function on social media apps, leaving 42.2% who cannot or are unsure. Knowledge of account recovery steps is fragmented: only 36.7% selected the comprehensive "all of the above" response for what to do if an account is hacked, and only 6.2% independently prioritised turning on 2FA, a finding consistent with the very low 2FA adoption identified in Section B.

The most concerning single finding in the survey appears here. In response to the statement "if I pay or send more photos, the problem will go away", only 67.4% clearly reject this belief (disagree or strongly disagree); 15.6% agree or strongly agree with it, and 17.0% are unsure. In other words, close to a third of respondents (32.6%) do not clearly reject a belief that is directly contrary to how sextortion cases are known to escalate in practice, once payment or further images are provided, demands typically continue rather than cease.

Awareness of formal support services is a further significant gap: only 37.7% know that helplines or support services exist for victims of online abuse, 36.9% do not, and 25.4% are unsure, meaning close to two in three respondents (62.3%) lack confirmed awareness of a formal support pathway. Where respondents would turn if something harmful happened, parents or guardians are the most nominated safest person to tell (35.2%), ahead of teachers or school counsellors (19.7%) and health workers or counsellors (7.0%). A small but real subset, 4.1%, would tell no one, indicating a group of respondents who may be effectively isolated from any support pathway. Finally, fear of blame is present in over a third of the cohort: 36.3% fear being blamed if they report online harassment, and 10.0% believe victim-blaming is acceptable outright, with a further 16.0% unsure (26.0% combined not clearly rejecting victim-blaming). Fear of blame is a well-established deterrent to disclosure in the broader harassment and abuse literature.

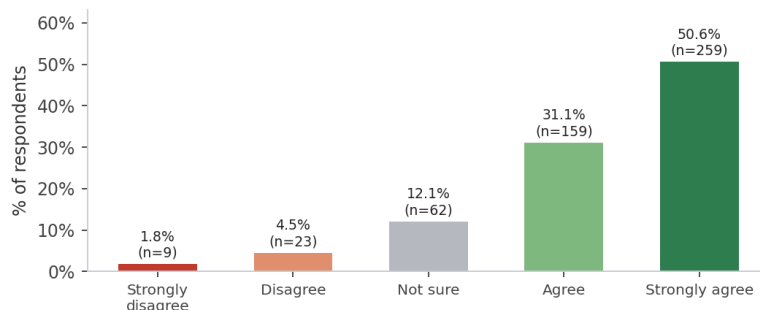
NEXT GENERATION AI RESEARCH CENTRE

Reporting and help-seeking pathway indicators



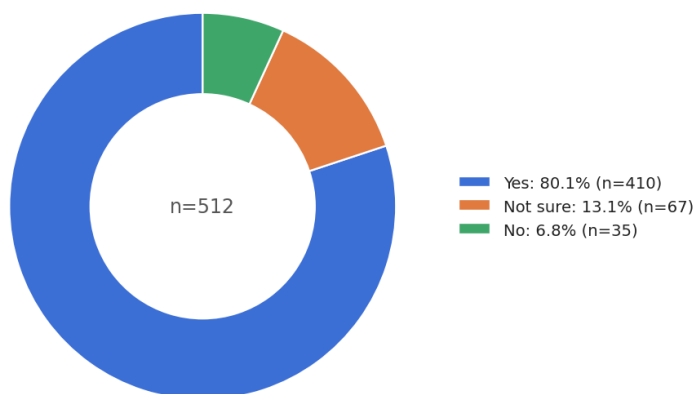
Overview 3. Reporting and help-seeking pathway indicators (n = 512).

Q24. "Everyone has the right to be safe online"



Q24. "Everyone has the right to be safe online" (n = 512).

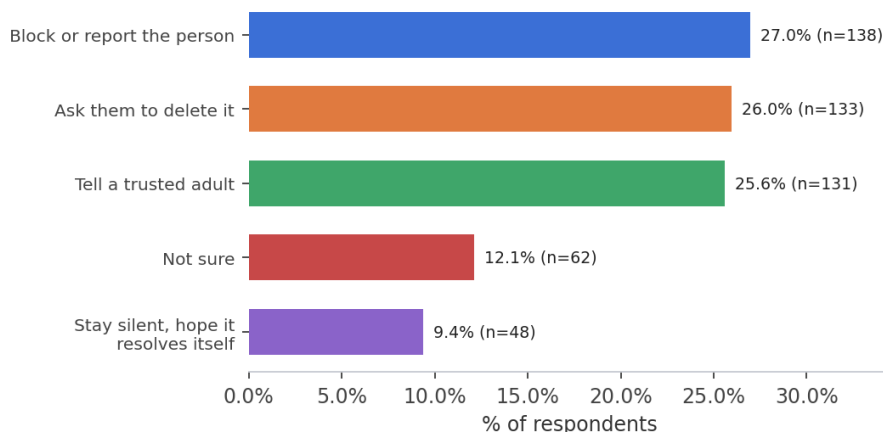
Q25. Posting someone's photo/video without consent is wrong



Q25. Posting someone's photo/video without consent is wrong (n = 512).

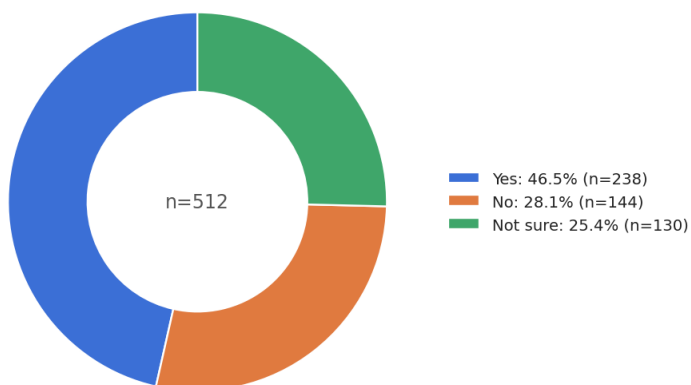
NEXT GENERATION AI RESEARCH CENTRE

Q26. First action if a photo/video is shared without consent



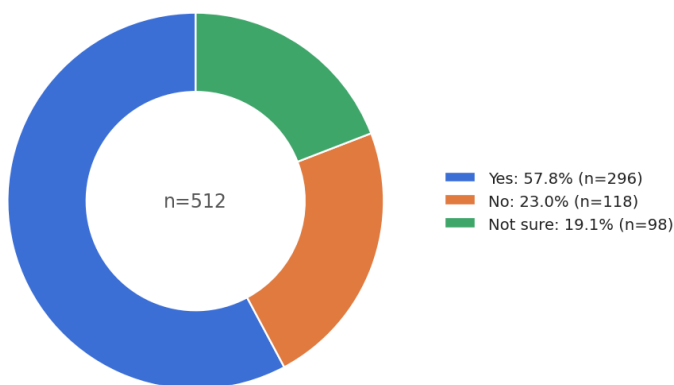
Q26. First action if a photo/video is shared without consent (n = 512).

Q27. Awareness that preserving screenshots/links/timestamps helps



Q27. Awareness that preserving screenshots/links/timestamps helps (n = 512).

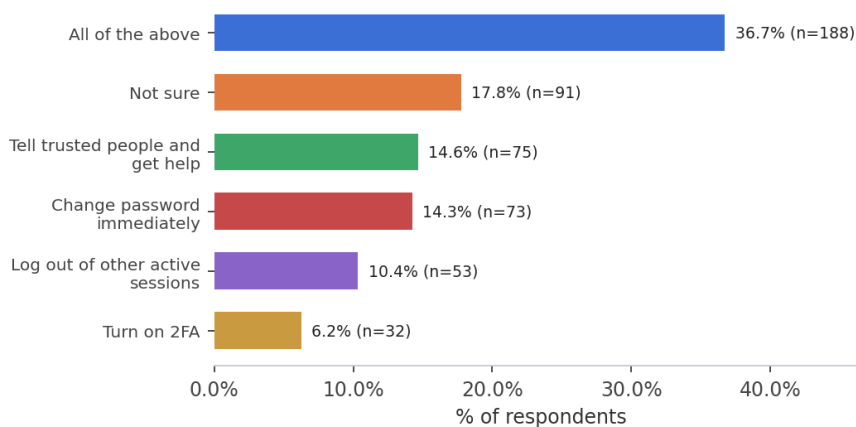
Q28. Confidence in locating and using the "Report" function on apps



Q28. Confidence in locating and using the "Report" function on apps (n = 512).

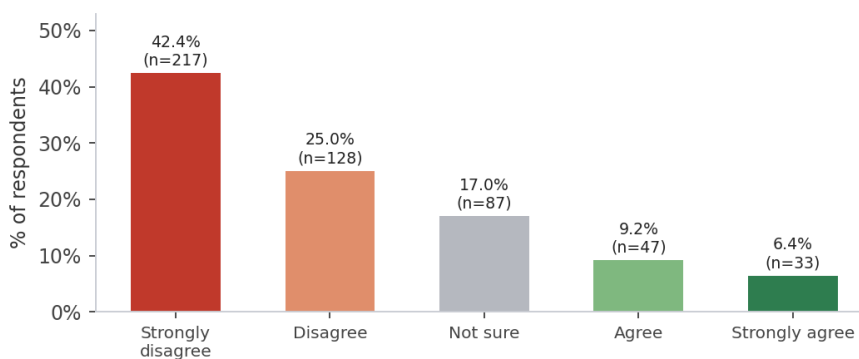
NEXT GENERATION AI RESEARCH CENTRE

Q29. First action if a personal account is hacked



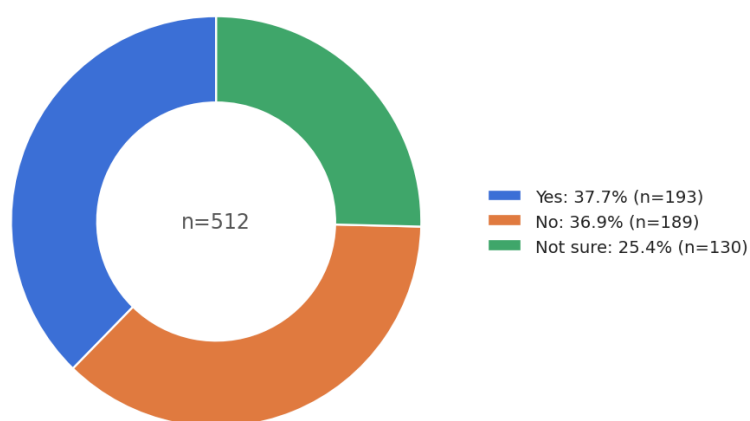
Q29. First action if a personal account is hacked (n = 512).

Q30. "If I pay or send more photos, the problem will go away"



Q30. "If I pay or send more photos, the problem will go away" (n = 512).

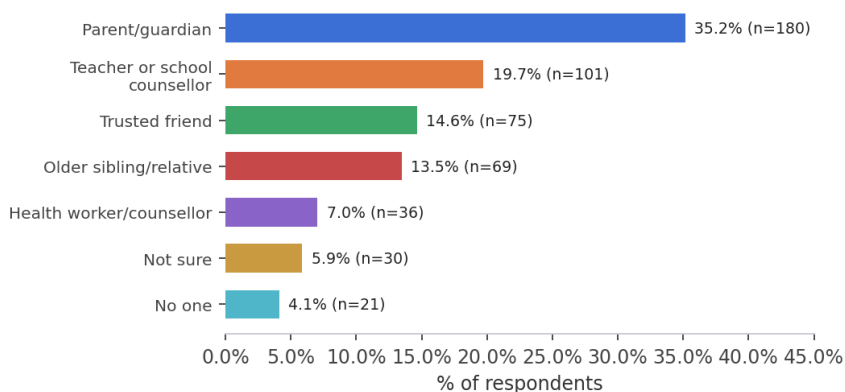
Q31. Awareness that helplines/support services exist for victims



Q31. Awareness that helplines/support services exist for victims (n = 512).

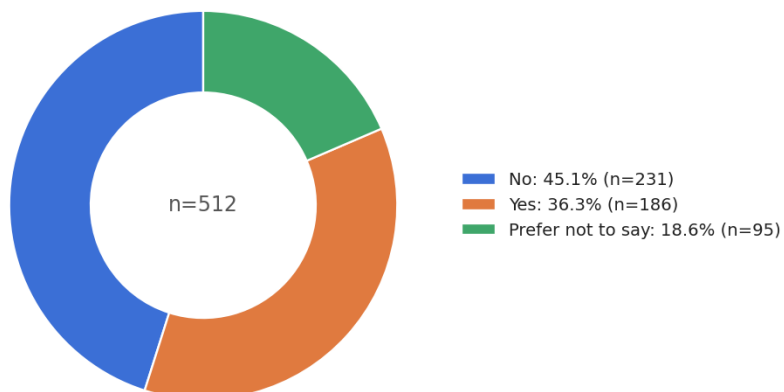
NEXT GENERATION AI RESEARCH CENTRE

Q32. Person considered safest to tell if something harmful happened online



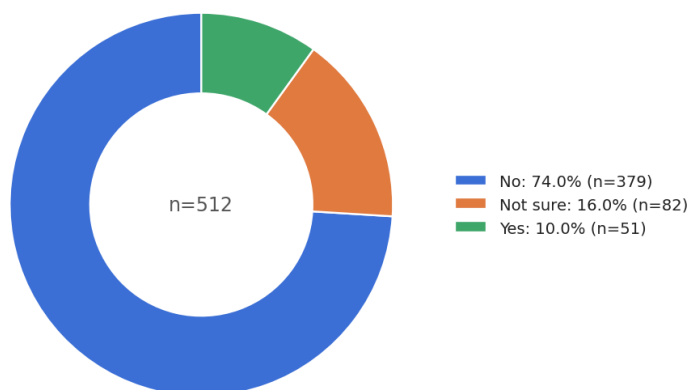
Q32. Person considered safest to tell if something harmful happened online (n = 512).

Q33. Fear of being blamed if reporting online harassment



Q33. Fear of being blamed if reporting online harassment (n = 512).

Q34. Belief that blaming the victim of online harassment is acceptable



Q34. Belief that blaming the victim of online harassment is acceptable (n = 512).

F. Responsibility & Online Behaviour

How students behave online, and what they value

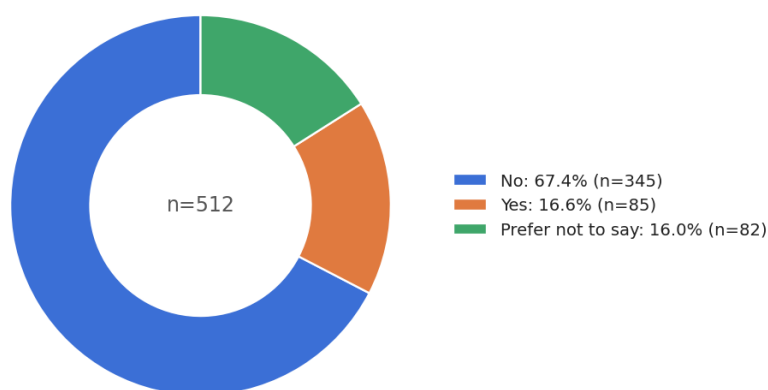
16.6% of respondents admitted to sharing someone else's photos or messages without permission, and a further 16.0% preferred not to say. Combined, close to a third of the sample (32.6%) either engaged in, or were unwilling to disclose engagement in, a behaviour that constitutes a form of the harm the survey otherwise asks about; this pattern is also consistent with the known tendency for self-report data to understate socially undesirable behaviour.

Bystander response to peer harassment shows a mixed picture. 24.6% would tell a trusted adult or authority, 24.0% would tell their friends to stop, and 22.7% would directly support the person being bullied. However, 17.0% would stay silent ("not my business") and 3.3% would join in, meaning approximately one in five respondents (20.3%) would either enable or disengage from a peer harassment situation rather than intervene or report it.

On content verification, 70.5% agree or strongly agree they have a responsibility to verify content is true before sharing it, a broadly positive finding, though the remaining 29.5% represents a meaningful pocket of susceptibility to unwitting amplification of misinformation or harmful content. When asked how they would respond if asked to forward someone else's private photo, 48.8% would refuse and explain why, and 36.5% would block or report the request. However, 6.6% would forward it, and 8.0% are unsure, meaning 14.6% either would comply with or are uncertain how they would respond to a request that facilitates non-consensual image sharing.

Consent literacy is the weakest single knowledge area identified in this section, and arguably in the survey given how frequently it recurs as an apparent determinant of other findings. Only 31.8% of respondents report a clear understanding of "consent" in the context of sharing someone's photo or information; 42.4% report only partial ("somewhat") understanding, and 25.8% report no understanding at all. Combined, 68.2% of respondents do not have a clearly stated understanding of consent, a concept that underlies several of the concerning findings documented earlier in this report (questions 26, 30 and 38). Interest in further learning across the six proposed topics is evenly distributed (14.1% to 19.7%), indicating broad-based demand for further education rather than a single dominant gap. Mental health support and safe help-seeking was the lowest-ranked interest area (14.3%), which, read alongside the low uptake of school counsellors as a disclosure pathway and the general support-awareness gap identified in Section E, may indicate lower salience of mental health support relative to other topics within this cohort's own stated priorities.

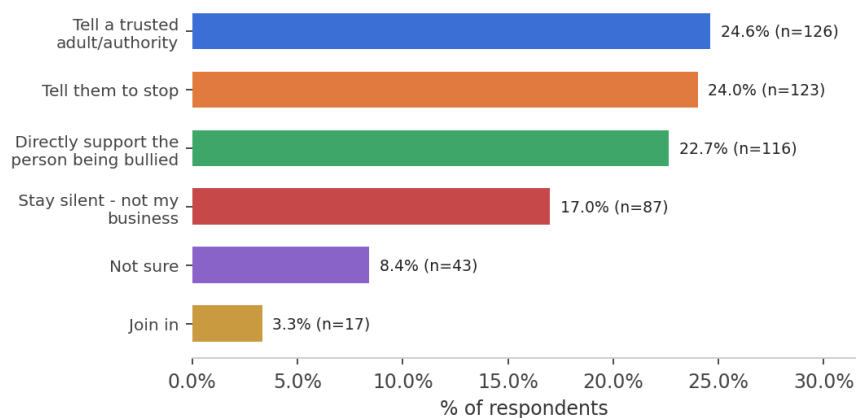
Q35. Has shared someone else's photos/messages without permission



Q35. Has shared someone else's photos/messages without permission (n = 512).

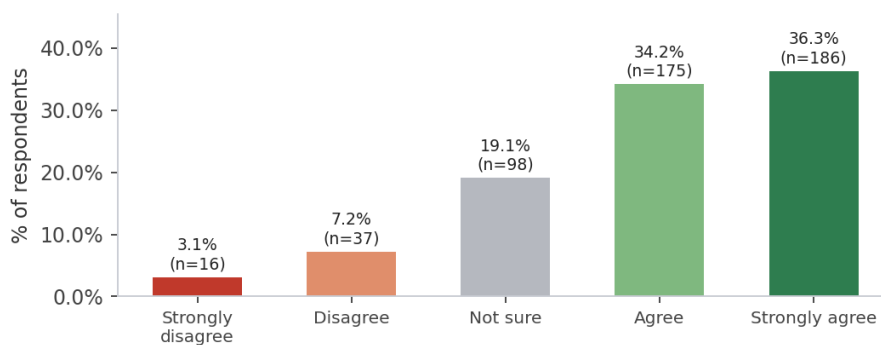
NEXT GENERATION AI RESEARCH CENTRE

Q36. Likely response if friends were bullying someone online



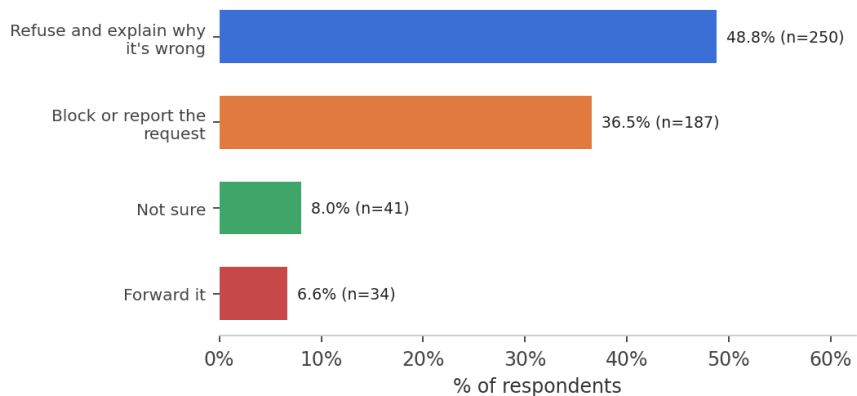
Q36. Likely response if friends were bullying someone online (n = 512).

Q37. "It is my responsibility to verify content before sharing"



Q37. "It is my responsibility to verify content before sharing" (n = 512).

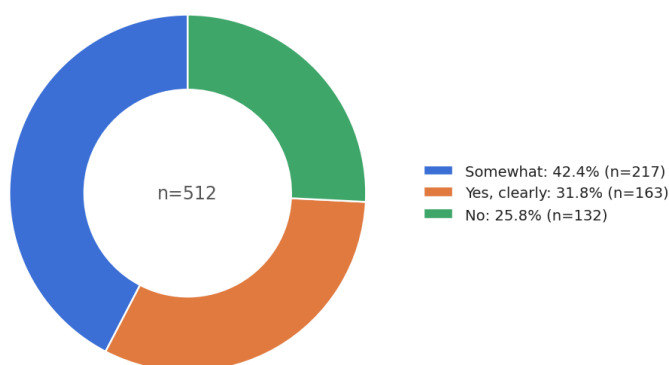
Q38. Response if asked to forward another person's private photo



Q38. Response if asked to forward another person's private photo (n = 512).

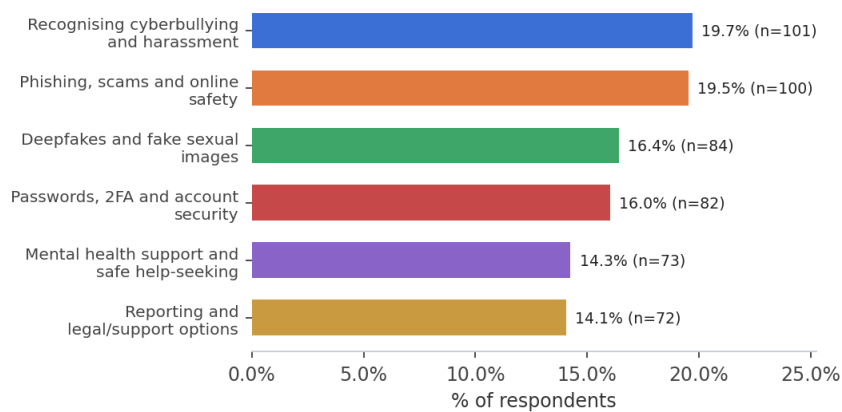
NEXT GENERATION AI RESEARCH CENTRE

Q39. Understanding of "consent" in the context of sharing photos/information



Q39. Understanding of "consent" in the context of sharing photos/information (n = 512).

Q40. Topic of greatest interest for further learning



Q40. Topic of greatest interest for further learning (n = 512).

Summary of Concerning Issues

Consolidated, cross-referenced list

The following list consolidates the concerning issues documented in this report, cross-referenced to the relevant survey section. It is provided as a reference summary only; issues are listed in the order they arise through the report, not in order of severity.

1. Weak and/or reused passwords combined with very low two-factor authentication adoption (Section B), indicating elevated risk of account takeover.
2. Limited profile privacy configuration and understanding, combined with over half the cohort not consistently verifying new online contacts (Section B), indicating elevated exposure to unsolicited contact.
3. Low awareness of the term and concept of online sextortion (Section C), within a population that sits directly inside the age range most frequently targeted by this harm category.
4. Limited awareness of AI-generated deepfakes relative to the survey's own coverage of fake imagery as a form of abuse (Section C).
5. High prevalence of direct or secondhand exposure to online harassment (52.7% / 48.6%), set against lower recognition of the issue's importance by close to a third of respondents (Section D).
6. Low rate of “tell a trusted adult” as a first response to non-consensual image sharing, and limited evidence-preservation knowledge, indicating a weakened incident-response and escalation pathway (Section E).
7. Close to a third of respondents do not clearly reject the belief that paying or sending further photos resolves an extortion-type demand (Section E).
8. Close to two in three respondents lack confirmed awareness of helplines or support services for victims (Section E).
9. Fear of blame, and residual acceptance of or ambivalence toward victim-blaming, present in over a third of respondents (Section E), a known deterrent to disclosure and reporting.
10. A bystander-disengagement or enabling pattern present in approximately one in five respondents when friends are bullying someone online (Section F).
11. Widespread incomplete understanding of consent (68.2% with partial or no understanding), a concept underlying several of the findings above (Section F).
12. Self-reported or undisclosed prior non-consensual sharing of others' content, present or unstated in close to a third of respondents (Section F).

This report has been prepared to surface and document concerning issues identified in the survey data from a cybersecurity and online safety perspective. Consistent with the scope agreed for this phase of work, it does not put forward recommendations or remedial measures. The next step in this process is for NGAIRC advisors to monitor, further analyse and interpret these findings in context, and to determine and provide an appropriate programme update.