State Comptroller | Special Audit Report | 2022

Protection of Minors on the

Online Space

Summaries

Background

The online space is a central arena of activity in the world of children and youth. They are active there for various needs, for increasing time, and from a younger age than in the past. The online space (Internet) provides children and youth opportunities to meet, communicate, and play, but also to harm and be harmed. Along with its inherent advantages, it holds many risks – including sexual abuse, bullying, and ostracism, disseminating pictures of a sexual nature without the consent of the person photographed, exposure to harmful materials, and more.

Harms and risks on the Internet

The risks inherent in the Internet are relevant to the entire population, but they increase concerning children and youth. The reasons for this include, among other things, the extensive use of the Internet by these age groups, the importance of social relationships at these ages and the centrality of social media in managing them, and emotional immaturity at these ages to contend with risks and harm.

The consequences of Internet abuse

Internet abuse of children and youth can have severe consequences, some of them long-term expressed socially, emotionally, and behaviorally. These include undermining self-confidence, increased risk of consuming drugs and alcohol, problems with studies and social frameworks, tension, stress, refraining from participating in social frameworks, and more.

Audit actions

From March to December 2021, the State Comptroller Office examined the protection of children and youth on the Internet regarding enforcement, treatment, education, and prevention. The examination was conducted at the National Child Online Protection Bureau – 105 Hotline (the National Bureau), the Ministry of Education, and the Israel Police (the police). Supplementary examinations were carried out at the Ministry of Justice, the Ministry of Public Security, the Ministry of Communications, the Ministry of Welfare and Social Affairs (the Ministry of Welfare), the National Insurance Institute, and the Tzur Unit in the Israel Prison Service. Furthermore, a dialogue was held with non-profit associations, organizations, and experts. In addition, a meeting was held with representatives of the National Council of Students and Youth. A public participation process was carried out with parents and principals (below – the parent and principal surveys conducted by the Office of the State Comptroller).

This audit report contains two parts:

Part one – protection of minors in the online space – the national effort

Part two – the Ministry of Education's actions to prevent harm to students on the online space

Part one
Protection of Minors on the Online Space – the National Effort

Background

To address the risks inherent in the online space (Internet) for children and youth, in 2016, the Government decided to establish the National Child Online Protection Bureau (the National Bureau). The National Bureau was established in 2018 as a combined police and civilian array dealing with Internet violence and crime against children and youth. The Israel Police, the Ministry of Public Security, the Ministry of Education, the Ministry of Health, and the Ministry of Welfare and Social Affairs participate, with the guidance of the Ministry of Justice. The Bureau comprises a police unit (Unit 105), which includes an intelligence division and an investigations division; the 105 Hotline staffed by police alongside representatives of the government mentioned above ministries; and a civilian department coordinating all of the civilian activity. Various government ministries and other entities work alongside the National Bureau regarding the prevention, treatment, and enforcement of protecting children and youth on the Internet.

Key figures

85.5%

of students in grades 6−12 own a smartphone[1]

about 4 hours

average daily smartphone use among children and youth[2]

28,623

incidents of harm to minors on the Internet were reported to the 105 Hotline from February 2018 to June 2021

11.5%

of students in grades 6, 8, and 10−12 in Israel were victims of Internet bullying, according to an international survey conducted in 2019.[3] (I.e., an estimation of about 75,000 students were victims of Internet bullying in the two months preceding the survey)

2,602

investigation files were opened due to Internet offenses in which the victim was a minor from 2018 to August 2021. Considerable rate (70%) were closed

1,216

investigation files were opened due to Internet sexual offenses in which the victim was a minor from 2016 to September 2021. Half of them were closed. About half (47%) of the victims in these cases were 12−14 years old

in 32%

of cases opened due to Internet sexual offenses, at least one victim was a minor

25%

of the victims in violations of the Videos Law cases are minors

1,498

pictures or video dissemination complaints were received at the 105 Hotline until September 2021. Most of the perpetrators and victims were 13−17 years old

---

1   Yossi Harel-Fisch, Noa Steinmetz, Riki Tesler, Rotem Maor, Meyran Boniel-Nissim, Sophie Walsh, "Youth in Israel: Patterns of Use of Addictive Substances, Involvement in Violence and Internet Violence, the National HBSC Study in Israel (2019) − Summary of Expanded Findings in the Areas of the Ministry of Public Security, Analysis of Trends between 1994 and 2019, and International Comparison," Bar-Ilan University, 2020 HBSC Survey).

Health Behaviors in School Aged Children (HBSC) A World Health Organization Cross-National Study.

2   Parent survey conducted by the Office of the State Comptroller in July 2021.

3   HBSC survey.

Key findings

🖓 **Lack of a national policy** – the international entities that deal with the issue and the 2016 government decision assert the need to formulate a national policy effectively contending with the challenges regarding the protection of minors on the Internet. As of October 2021, the inter-ministry steering committee had not yet formulated a national policy. With no policy defining national objectives, determining areas of activity and clear targets for each of the stakeholders operating in the field, defining the target audiences to work with, and addressing the resources and budgets necessary for implementing it in the short and long term – the ability to address the issue optimally is undermined.

🖓 **Introduction to the 105 Hotline** – by an HBSC survey from 2019 most children and youth harmed on the Internet (70%) did not report it. By the Ministry of Public Security survey in 2019, a significant percentage of the participated youth (41%) had not heard of the Hotline. By the State Comptroller Office survey among parents in July 2021, 51% of parents who participated in the survey had not heard of the Hotline.

🖓 **Service in the Arabic language** – one in ten calls to the 105 Hotline is in Arabic. Among them – are calls related to the dissemination of pictures and videos of a sexual nature or those that might harm the minor due to photographs not compatible with dress or behavioral patterns in conservative societies. As of August 2021, there were no Arabic-speaking police officers at the Hotline. To handle these calls, the Hotline received the help of a representative of the Ministry of Education and Arabic-speaking police officers from other districts who volunteered to help. As of November 2021, a police officer who underwent several months of Arabic language training is serving at the Hotline. These solutions are not optimal.

🖓 **Online contact** – children and youth are active on the Internet and usually communicate using various applications (such as chat and WhatsApp). By the survey, about 45% of them preferred to complain against Internet abuse cases through online means. Nevertheless, as of November 2021, the only way to reach the Hotline is by phone.

🖓 **Lack of data on calls referred by the Hotline to be handled by police stations** – 56% of the Hotline calls are classified as criminal incidents. These incidents are usually referred to be handled by police stations. It was found that neither the Hotline, the National Bureau, nor the police had data on the number of calls referred by the 105 Hotline to police stations over the years.

🖓 **Effectiveness assessment of the Hotline enforcement activities** – the Hotline locates suspects and issues warrants to help the police stations handle the investigation files. It was found that the Hotline does not receive systematic and

organized feedback from the stations regarding calls about Internet offenses against minors it has referred to them (for example – if a criminal case is opened or has been closed, and if so – on what grounds, and what difficulties the investigators encountered).

👎 **Comparing the investigation files opened at the stations with those opened following a call to the 105 Hotline** – the State Comptroller Office received from the 105 Hotline a partial list of the calls it had referred to police stations and analyzed their handling at the stations. The analysis indicates a need to thoroughly examine the effectiveness of the Hotline enforcement activities, as well as the stations' difficulties handling Internet-related files:

- **Lack of a criminal offense –** about a quarter of the investigation files opened at the stations following calls to the 105 Hotline (441 out of 1,704) were classified by them as "general cases" and were closed as they did not include a criminal offense. This is even though the stations opened then following an initial examination by a police officer at the 105 Hotline. Therefore, it raises a concern that a criminal offense was committed.

- **An almost identical percentage of cases closed – 71%-72% –** notwithstanding preliminary actions at the 105 Hotline, the rate of cases closed is almost identical between cases where the complaint is received directly at the station and those that followed a call to the Hotline (72.3% vs. 71%). Nevertheless, there are differences in the grounds for closing them – the percentage of cases closed on the grounds of "unknown offender" is lower in cases originating in calls to 105 (about 34% compared to 51%).

👎 **The technological systems at the 105 Hotline –** for about three years, the 105 Hotline has been operated using inadequate technological systems. As a result, the handling quality of incidents is affected, it is challenging to supervise and monitor the handling of incidents, and there is a constant concern about mishaps. It was found that only in August 2020; NIS 2.7 million was transferred to develop the technological systems adapting them to the 105 Hotline's activity.

👎 **Filtering harmful content –** the provisions of the law require Internet access providers to inform their subscribers of dangerous websites and content and offer them a filtering service at no cost. Supervision by the Ministry of Communications raised that the companies usually did not fulfill this obligation (80%-100%). Furthermore, by a survey conducted by the State Comptroller's Office among parents in July 2021, about a third of them did not know about this service.

👎 **Enforcement aspects – the lack of a situation assessment of the Internet crime scope –** it was found that despite the increase in the Internet crime scope, the enforcement bodies – the Israel Police and the State Attorney's Office – have no data to reliably estimate the online crime scope, its trends in general, regarding minors in particular. This result stems from three main reasons:

a. **Classifying investigation files as "Internet related" by the Israel Police –** the police classifies online offense cases as "Internet related" when opened at the police station. However, many cases were classified is incorrectly, affecting the police's ability to identify processes and phenomena in online crime. For example, out of 1,263 cases originating at the 105 hotline, 502 (40% of the cases) were not classified at the stations as "Internet related" even though that is the Hotline focus.

b. **Not classifying cases as "Internet related" by the State Attorney's Office –** it was found that the State Attorney's Office's computer systems, had no field that deals with committing an offense in the Internet. As a result, it is impossible to retrieve automatically data from the Office's systems on cases opened due to online offenses[4] and indictments filed about them.

c. **Lack of information on victims who are minors in the State Attorney's Office's systems –** it was found that it is impossible to retrieve exhaustive or reliable data from the State Attorney's Office's systems on the minors victims' number in general and on those harmed online in particular.

🖓 **Examining the police handling of a list of Internet pedophilia suspects –** in 2019, the police compiled a list on 190 potential suspects of being involved in committing Internet pedophilia offenses based on the information that the police had; the suspects were classified according to their dangerousness. In February 2020, the list was distributed to all units at the police. Since the distribution, the police have not dealt with 31 suspects (out of 108 suspects classified as the most dangerous) overtly or covertly, even though they were classified at the highest level of dangerousness.

🖓 **Dissemination of sexual pictures and videos of a person without consent – the Videos Law – awareness among youth –** many youths are seriously harmed by the dissemination of photos and videos of a sexual nature. By the Videos Law, committing such harm is a criminal offense, and thus youths can find themselves breaking the law, with all this entails. Surveys indicate that many of them (about a third) are unaware of the law.

🖓 **Gaps at the police stations –** the expansion of crime to the Internet pose significant challenges to law enforcement bodies, including exhausting digital evidence. Difficulties were found in the technology arena units'[5] activity, such as the increasing strain on technology arena investigators, obligated to serve all the station investigations; a lack of unloading stations to produce digital evidence at the station – both resulting in "traffic jams" and delays. This problem is accentuated given the enormous memory capacities each device has today, which prolongs the time needed for unloading and

---

4   Except in cases involving a specific offense category that relates to online activity.

5   Technology arena rooms in which trained investigators are stationed whose job is to help produce digital evidence – such as photos, videos, messages and correspondence – that are caught in digital devices such as computers, tablets, smartphone and cameras.

producing the evidence; this tremendous amount of digital evidence requires special storage and analysis taking a long time, given the significant amount of information accumulated. These difficulties cause delays in handling all investigation files, including those involving online offenses against minors.

In addition, gaps were found regarding the ability of youth units at the stations to address online youth crime. Among other things, by the police documents, youth investigators are unfamiliar with the language of the investigated children and insufficiently familiar with the online space. They cannot investigate cases that demand many resources and technological skills.

The National Bureau – the 105 Hotline – the National Bureau is a unique model in Israel and worldwide. Cooperation between the police and representatives of the various government ministries enables holistically addressing harm to children and youth on the Internet. Naturally, this model is challenging and demands coping with complexities that stem from working side by side to workers from different organizational cultures and employment conditions. It requires solutions on the hierarchical level within the work model. The National Bureau has contended with its challenges, and constant consideration is needed to ensure optimal performance within this model.

Key recommendations

- It is recommended that the inter-ministry steering committee formulate of a long-term national policy. Setting out a policy guiding the many stakeholders involved, including the National Bureau, the Israel Police, and the various government ministries, will optimally address its inherent challenges, chiefly those defined in the threat reference. This policy will be examined from time to time considering technological developments and changes in the risk map.

- For Internet abuse victims to contact the Hotline, they must be aware of its existence. It is recommended to further invest in publicity efforts and consider the most effective ways to raise awareness of its activity.

- It is recommended that the Israel Police and 105 Hotline examine in depth why the percentage of cases closed at the stations is identical (about 70%), whether the complaint was received directly at the station, or whether it followed a call to the Hotline.

- The 105 Hotline began operating in 2018 and has handled over 28,000 calls since then. The 105 Hotline model is unique. To evaluate the service the Hotline provides and its

effectiveness by the callers' part and to improve its activity, it is essential to receive feedback from the public regarding its service. It is recommended that the National Bureau receive such feedback.

To enable a reliable situation assessment of online crime and to derive insights from it, it is recommended that the Israel Police and the State Attorney's Office examine how to improve the classification of cases in which offenses have been committed online.

Given the high level of dangerousness determined regarding 31 suspects included in the pedophilia list the police compiled, the police should investigate the suspicions, overtly or covertly, regarding all of the suspects, and in particular, those the police defined as a high level of dangerousness, alongside its handling of other suspects. Furthermore, it is recommended that the police periodically follow up on the issue with the various police units to ensure maximum police attention towards suspects of pedophilia at the most severe level. It is also recommended that the police consider implementing continued follow-up in the coming years.

The Ministry of Education should increase awareness of the Videos Law and its consequences and consider including it in the curriculum. In particular, it should be a mandatory topic in middle schools. Given the severe harm to the person whose photo has been disseminated to the public without consent, the Ministry of Education should emphasize to youth that alongside their right to send photos and videos of themselves to others, they must be aware their photos might be disseminated to others and their control over the photos will be lost.

Investigative bodies face significant technological challenges when fully utilizing digital evidence, affecting the conduct of investigations in the online space; these will intensify as technology develops and as online crime increases. These challenges require suitable technological response enabling complete, optimal, and quick utilization of digital resources. The Israel Police should consider the difficulties regarding the activity of the technology arena rooms at the stations and examine the unique needs and response to bridge the technological gaps that hamper investigative activities. This is underlined as fully utilizing digital evidence is necessary today in many investigation files, not just to online crime.

Abstract | **Part one - Protection of Minors on the Online Space – the National Effort**

Statements that were made in a dialogue with National Council of Students and Youth representatives

There is almost no one who has not **experienced sexual** harassment, both boys and girls – it crosses sectors and sexes • No one has not **experienced sexual** abuse in the virtual realm, and many times, there is no knowledge about how to cope with it • Even if I block a harasser, **a week later, another harasser will come** • **There are not enough tools to cope with it** • I am exposed to **shocking videos** on the internet • Spending a lot of time on the Internet • Children's time in front of a screen exposes them to harmful content • Prolonged use of the internet is essentially an addiction • There is a lot of **impersonation** on the internet and even **faking conversations** of a harmful or sexual nature • Gambling on the internet by youth • We have all encountered and know youth who have been harmed • In your immediate environment, within 5-10 minutes, you can get **cannabis and alcohol**, and the internet has made it highly available and accessible • **Ostracism on the internet** reaches more people and stays in the virtual space for a long time • You can put photos there, and anyone can be anonymous and write what they want • **Ostracism on the internet is much crueler**, and it stays there • Advertisements with thin women and tall men **hurt self-confidence** • **High exposure to drugs on social networks**
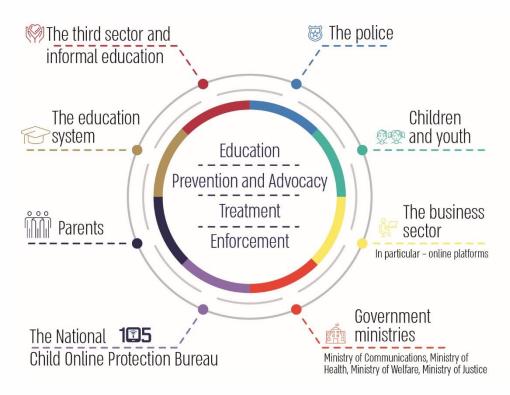
Summary

The online space offers abundant opportunities for children and youth, but, the more they are exposed to a wider variety of uses and options, the more they are exposed to risks and harm inherent in the online space. These harmful consequences can be severe and affect the victims for many years.

The National Bureau is a unique combined civilian-police array providing a holistic response to Internet abuse of children and youth. The police and government ministry representatives at the National Bureau, particularly at the Hotline and in the operational unit, work out of a sense of mission, and are exposed to sensitive information, which requires emotional resilience. Establishing the National Bureau is a significant step in addressing the issue. Still, additional measures are necessary to cope with the Internet's challenges, with its constantly changing risk map.

This report presents a series of gaps, including the lack of a national policy for the protection of children and youth on the Internet; the absence of a situation assessment on online crime scope; gaps in the civilian and law-enforcement Hotline activities; and gaps in the police stations' handling of online offenses. Addressing these gaps will improve the national effort to protect children and youth on the Internet.

Many entities are involved in the Protection of minors online – children and youth and their parents, the National Child Online Protection Bureau, the formal education system, informal education, law enforcement, and relevant government ministries, including the Ministry of Education and online platforms and third sector organizations. Every solution concerning the responsibility of one entity in this complex equation will ultimately be partial and insufficient. Addressing online risks requires broad action on the national level, including handling aspects of education and prevention, treatment and enforcement, and enlisting all relevant stakeholders in coordinated action on this important issue.

The third sector and informal education

The police

The education system

Children and youth

Education
Prevention and Advocacy
Treatment
Enforcement

Parents

The business sector
In particular – online platforms

The National 105 Child Online Protection Bureau

Government ministries
Ministry of Communications, Ministry of Health, Ministry of Welfare, Ministry of Justice

In a work model where several government ministries work shoulder-to-shoulder to provide a holistic solution, there are significant advantages for coping with problems across ministries. It is also worth examining the implementation of this model in other areas in which there is a clear advantage in joint handling by staff from different ministries.

Part two
Ministry of Education actions to prevent harm to students on the online space

Background

The Ministry of Education (the Ministry) explicitly addresses online space (Internet) abuse and getting involved in risky Internet situations as part of students' violence towards students. Under its authority, according to the law[6], the Ministry of Education is responsible for advancing an optimal educational climate that enables including and accepting others and encourage the creation of an atmosphere that supports learning and the development of personal and social responsibility. The Student's Rights Law 2000 intends to reduce violence between students in and outside educational institutions.[7] A Director-General circular on improving the school climate and coping with incidents of violence[8] (the ACHAM circular) is based on the concept that the school climate is central to develop students' self-confidence, their sense of belonging, and their dignity, alongside social values such as integrity and respect for others, responsibility, protecting the privacy and being alert to dangers and risk situations. However, students' behavior in the online space has unique characteristics: access to extensive information and to diverse content that is unlimited and unclassified, blurring the boundaries between private and public and risk of violating privacy, the possibility of anonymous and independent behavior without the supervision of teachers or parents and monitoring mechanisms. These characteristics pose a new educational challenge to all levels of the education system, which requires planning and preparation exceeding the Ministry of Education's response to physical violence and risk behaviors visible to students.

---

6   The State Education Law 1953 and Compulsory Education Law 1949 make it mandatory for the state and for local authorities, which are local education authorities, to maintain educational institutions for every child and for every youth and to report any incident of violence between a teacher and student or between students; and Government Decision no. 1006, on the topic of "the establishment of a framework for preventing violence and crime against children and youth on the internet (Maor framework)", from January 17, 2016, which was updated on November 18, 2018, for establishing a civilian-police framework that will work to create a safe environment for children and youth online – a framework in which the Ministry of Education is a partner and takes an active part in the civilian framework.

7   As for the Ministry of Education's responsibility for the activity of students outside of the educational institution according to the law, see Pupils' Rights Law, 2000, according to which the Ministry is also responsible "for the rules regarding maintaining mutual respect in the community of the educational institution…including regarding preventing violence and addressing it."

8   See Director-General circular "Optimal Educational Climate and Educational Institutions' Coping with Incidents of Violence and Risk" from May 21, 2020: "The updated circular… expands the scope and defines the authority of the educational staff on additional issues that did not appear in previous circulars, such as incidents of violence that take place outside of the educational institution or on school buses… and creating partnership with parents."

Key figures

9% vs. 22%

the level gap of online violence towards students ranges from 9%, according to a violence monitoring survey by the National Authority for Measurement and Evaluation in Education (RAMA), and 22%, according to Bezeq's Internet report

50%

of all schools, principals stated they could rely between a medium level and not at all on the Ministry of Education to provide a quality and professional response protecting minors on the internet

35%

of all schools, principals stated that the current internet programs distributed by the Ministry's headquarters provide students with tools for Internet safe use – both as part of school activity and in leisure hours – at a medium level or below

25%

of parents of students in the Jewish-state education system think they have tools to reduce exposure to problematic content on the internet

50%

of middle school and high school, students do not consider school staff as people they can turn to in case of online violence. Over 60% of students in these age groups do not address the 105 Hotline in case of online violence

70%

of all school principals reported their school does not have programs dealing with students who harm others on the internet; 58% said there are no programs for helping students who have been harmed on the internet

83%

of parents stated they did not participate or were not invited to participate an in safe internet use activity at school

22%

of all schools, principals indicate that their school only slightly uses or not at all the monitoring tools that the Ministry of Education provides them with to build the system-wide school program[9]

---

9   In the "principles for preparedness" section, the Acham circular states among other things that each school must develop an ongoing and consistent system-wide program that is a necessary condition for creating a safe environment; the program should be based on monitoring violence, its extent and its nature at the school.

Key findings

🖓 **Integrating the issue as a target in the education system's strategic planning** – in May 2020, the Ministry's headquarters formulated a system-wide multi-year plan for promoting optimal behavior by students and preventing harm to them on the Internet. Still, as of October 2021, it had not yet been approved by the Ministry's director-general nor distributed to the districts and educational institutions. It was also found that the Ministry did not set any supervision, monitoring, and reporting tools for its implementation in the plan.

🖓 **Performance planning and regulation – director-general circulars and curricula for promoting optimal behavior by students on the Internet and preventing harm to them** – it was found that the psychological counseling service in the Ministry of Education's pedagogical administration (SHEFI) has not updated the director-general circular on life skills from December 2010 (the Life Skills Circular). In the director-general circular, there is no explicit reference to the Life on the Internet Program – the designated operative program for ensuring optimal behavior on the Internet by students and preventing harm to them on the Internet (the Life on the Internet Program). In the Life Skills Circular, there is no reference to components of the system-wide multi-year program for promoting optimal behavior on the Internet that SHEFI developed as a response to the set objective for promoting it in the strategic plan for the 2020−2021 school year. It was also found that the Ministry of Education's headquarters units are not tracking the implementation of the Life on the Internet Program and do not periodically assess it and update it as needed.

🖓 **Implementing the ACHAM circular,[10] the Life on the Internet Programs, and the Life Skills Program at schools** – most principals (85%) are familiar with the current internet documents the Ministry's headquarters has distributed. However, a large portion of them (over 40%) believe that the tools and programs they are running provide students with a medium or lower level of effective tools for coping with harmful incidents on the internet. In addition, only half of all school principals believe they can rely, to a great or very great extent, on the Ministry of Education to provide a quality and professional response to protect minors online, and about half (46%) stated they only use the monitoring tools the Ministry of Education provides them with between a medium extent and not at all. It was also found that from the 2018−2019 school year until the 2020−2021 school year, the number of schools that filled out and used the Acham questionnaire declined from 505 to 372 (255 Hebrew-speaking schools and 117 Arabic-speaking schools). In the 2020−2021 school year, 7.5% of all schools used the Acham questionnaire (372 out of 5,011).

---

10   See Acham circular.

👎 **Data collection by schools and compiling them at the district level** – the Ministry of Education's districts collect data on internet abuse from all schools in various ways and to varying extents. This data is kept at the district level, and the districts are not obligated, according to the Acham circular, to transfer it to the headquarters. As a result, the Ministry's headquarters does not have information compiled on incidents of online harm reported to school educational staff. It was also found that a third of all school principals stated that in the last school year, 2020−2021, they did not collect data on internet abuse; 21% of all school principals said this year there were no online violence, and 43% of all school principals stated that there were students who harmed other students on the internet in this school year.

👎 **Underreporting by students on Internet abuse and being in risk situations** – according to a digital violence monitoring survey by RAMA[11], 93% of students reported that they would turn to someone (not necessarily a school figure) if they experienced harm on the Internet. In contrast, turning to a school staff member stood at 57%: 70% of students in grades 4−6 would turn to a school staff member, compared to 44% of students in grades 10−11. If harmed, the percentage of students who would turn to the 105 Hotline (39%) was the lowest, especially as the student's ages increased. As for differences between Hebrew-speaking and Arabic-speaking students – 94% of Hebrew-speaking students, compared to 89% of Arabic-speaking students, reported that they would turn to someone (not necessarily a school staff member) if they experienced harm on the internet. In contrast, turning to a school staff member stood at 54% among Hebrew-speaking students compared to 65% of Arabic-speaking students. Moreover, 37% of Hebrew-speaking students and 45% of Arabic-speaking students stated they would turn to the 105 Hotline. In a meeting held by the audit team with representatives of the National Council of Students and Youth in August 2021, the students attributed the underreporting to the lack of entity that can address their complaints– inside or outside schools.

👎 **Coping with harmful incidents on the Internet towards students and by students** – according to principals' reports, about 70% of schools do not have programs for dealing with students who harm others on the Internet, and 58% of schools do not have programs for helping students who are harmed on the Internet. Half of all school principals reported they do not have adequate programs for dealing with students who harmed others or were harmed, and a third of all principals estimated that the treatment provided to students who were harmed or harmed others on the Internet was at a medium level or below.

👎 **The professional development of teachers** – only a third of all principals believe to a great extent or a very great extent that teachers have sufficient digital skills to help students use the Internet optimally and cope with incidents of harm, and the majority (76%) prefer that professionals with specific expertise teach the students in class.

---

11   RAMA, "Digital Violence at Schools According to Student Reports," September 2020.

Parent positions regarding guidance for parents – the Life on the Internet Programs, the knowledge extraction document initiated by SHEFI[12], and the National Child Online Protection Bureau raised the need for schools to cooperate with students' parents, guide them, and involve them in the issue. However, only about, a quarter (27%) of parents believe to a great or very great extent their children are exposed to inappropriate content or to harm on the Internet. As the age of children increases, parents are less involved in their Internet activity; 83% of parents stated that they had not participated in or were not invited to participate in an activity on safe Internet use at school. Hence, only about 17% of parents participated in activities on safe Internet use[13].

Including the issue as an objective in the Ministry of Education's strategic planning – at the end of August 2021, before the 2021–2022 school year, the Ministry published a policy document titled "Milestones for the 2021–2022 School Year", which was for all position holders in the education system, designated to plan this school year. The document was published on the education institutions portal and includes five goals. The second goal is "strengthening resilience and sense of belonging through emotional and social learning", and one of its goals is "advancing protection, preventing violence and bullying in educational institutions and the online space".

The impact of the COVID-19 pandemic on the extent of schools engaging in education on optimal behavior on the Internet – it was found that 63% of all principals estimate that due to the COVID-19 pandemic, their school was more engaged in educating students on optimal behavior on the internet. According to the principals, 70% of state-religious schools and 69% of elementary schools increased their involvement in the issue.

Updating teacher-training plans – the new teacher-training plan, approved by the Council for Higher Education in February 2021, includes eight core elements. It was found that two of them refer to protecting minors online and implementing learning technologies in online space[14]. Regarding the protection of minors, the work of the teacher and educator includes behavior on the internet and sex education. Learning and teaching technologies are included in entrepreneurship and innovation in learning information-intensive environments with diverse technologies.

---

12 Irit Aizik, Zohar Sharvit, Shakked Lubotzky-Gete and Dana Brender, "Promoting Safe Behavior on the Internet among Students – Literature Review and Extraction of Knowledge from School Programs," Myers-JDC-Brookdale, June 2020. Document developed with the help of SHEFI.

13 A third of parents stated that they had received an invitation to participate in activity at school, half of whom stated that they had participated in activities – that is, 17%.

14 Page 9 of the plan, "Expert Committee Report on Examining the Structure and Outline of Teacher Training in Institutes of Higher Education in Israel", April 2020.

Key recommendations

- It is recommended that the Ministry of Education validate and approve the multi-year plan for promoting students' optimal behavior on the Internet and preventing harm to them on the Internet developed in May 2020, distribute it to the districts and schools, and clarify the strategic direction and what the individual tasks and targets are for achieving it.

- It is recommended that the Ministry of Education discuss the significant gaps in the data received from the various monitoring tools regarding digital violence and risk situations on the Internet for children and youth, assess the reliability of the monitoring tools as a basis for formulating intervention programs for the variety of student ages and populations, and consider to update and validate them.

- To create a system-wide situation assessment including both the data from the National Child Online Protection Bureau and from the Ministry of Education's districts, it is recommended that the Ministry of Education regulate data collection from the districts in the Acham circular to uniform and reflect the data from the field, and that the circular obligate the districts to periodically report the data it has on Internet abuse to the Ministry's headquarters. In addition, it is appropriate that the Ministry of Education formulate a director-general circular on the information transfer about students, among other things, to determine clear rules regarding the confidentiality of information about students involved in online abuse, as well as ensure the continuity of dealing with them and preventing harmful behavior by them in the future. It should be noted that such a recommendation was included in the State Comptroller assessment submitted to the Knesset on "the implementation of the Prevention of Sexual Harassment Law, 1998"[15].

- To improve the response to students harmed or who have harmed others on the Internet, it is recommended that the Ministry of Education examine the scope of programs in schools for dealing with these students and adapt the response to their needs, and increase its cooperation with external groups – parents, local authorities and informal frameworks of student activities staff.

- By the responses from ultra-orthodox sector school principals, only about half a percent of students reported having been harmed on the Internet; it is recommended that the Ministry develop tools for principals and the educational staff to identify and help students harmed on the Internet compatible with the lifestyle of ultra-orthodox society inside and outside of schools.

- To expand the teachers' professional development, it is recommended that the Ministry of Education, in cooperation with the Centers for the Development of Teaching Staffs

---

15   State Comptroller, Annual Report 70b (May 2020) p. 111.

and representatives of teachers and principals, consider improving the professional development of teachers for teaching safe behavior on the Internet and closing the gap between them and students in this field.

💡 Given the great importance of the involvement and enlistment of parents to ensure optimal behavior of their children on the Internet, it is recommended that the Ministry of Education examine the quality use of tools by schools it provided for that end. It is also recommended that the Ministry make tools developed in this field accessible to parents and identify the barriers to the involvement of parents of students of various ages and from different population groups.
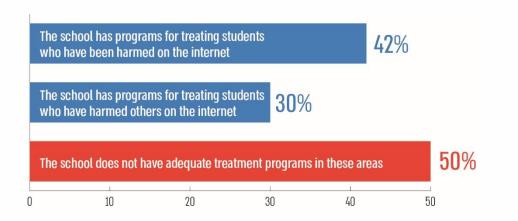
Statements from dialogue with Council of Students and Youth representatives regarding dealing with harm to students on the Internet

I think that school staff does not understand there is harassment on the internet... Parents who do not know how to cope with the phenomenon get stressed immediately and turn to the police, and the police do nothing... The youth who wants to complain has to be exposed, and there is **nothing the parents or school counselor can do, and they do not have tools for coping with it •** I think the school counselor does not have the means to synchronize with all those who are supposed to deal with it • I feel uncomfortable approaching the counselor of the grade, responsible for about 450 students • I want the possibility of turning to someone who will keep it between us • Everyone refers to everyone and leaves the youth to cope with it alone • **Therefore, everything ends with "learn to cope"** • I think the most important thing is for the harmed **person to have the possibility of speaking with someone** • You need someone trained to talk with those harmed at school or outside • Currently, **there is no clear address to turn** to stop the abuse reported by the youth.

Source: the audit team's meeting with representatives of the National Council of Students and Youth on August 2, 2021.

Treatment programs for students who have harmed others and for students who have been harmed on the schools' internet

The school has programs for treating students who have been harmed on the internet — 42%

The school has programs for treating students who have harmed others on the internet — 30%

The school does not have adequate treatment programs in these areas — 50%

0 10 20 30 40 50

Summary

The behavior of children and youth online has posed one of the most significant education system problems for over a decade. Alongside the education system obligation to instill its graduates with knowledge, tools, and skills preparing them to be "digital citizens," enabling them to integrate into life circles and the changing labor market, it should address the many risks inherent in students' intensive use of the Internet – a space that has become very central in their lives – at school and outside of it. Moreover, the Ministry of Education has a significant role in educating children and youth, preventing them from getting into risky situations on the Internet and treating those harmed. The Ministry of Education should advance these aspects in the pedagogical, emotional, moral, and organizational spheres.

In its response to the State Comptroller Office, the Ministry of Education presented a series of actions it has carried out over the years to advance optimal behavior on the Internet and prevent harm to students, including coordinating on the inter-ministry level until the establishment of the National Child Online Protection Bureau; active participation in the 105 Hotline; addressing various aspects, such as educational lectures at the 105 Hotline for about 3,000 school principals in the 2020−2021 school year; collaborations with various bodies (such as the State Attorney's Office and the police) to hold activities in the education system; and carrying youth leadership activities as part of the Peers Influencing Peers program that about 8,000 youth participate in. Furthermore, the Ministry of Education developed professional training for the educational staff, supervisors, and instructors, promoting optimal behavior on the Internet and increasing awareness of risk situations and harm at schools.

By the report's findings, the Ministry of Education has not created educational infrastructure at the level of the headquarters and the schools sufficiently addressing various aspects of optimal behavior on the Internet. Regarding the headquarters, several deficiencies were found regarding enacting the prioritized strategic status of the issue; enlisting all of the Ministry's headquarters units responsible for developing and implementing it; updating the procedures and programs and tracking their implementation; the insufficient professional development of teachers was also found; and failure to address gaps in monitoring and collecting the data on online abuse. The preparation and implementation of director-general circulars and plans are insufficient at schools, in contrast with the online space's dominance among students.

It is recommended that the Ministry of Education promote optimal behavior on the Internet to prevent harm to students by conveying its importance to all bodies involved in the education of students. Hence, it is recommended that the Ministry of Education expand the cooperation between the headquarters units and the field, clarify and update procedures and programs for building the infrastructure addressing the issue at schools, and increase the tracking of their implementation and the evaluation of their contribution. In addition, it is recommended the Ministry increase the involvement of parents to make it built-in. It should enhance the skills of teachers from the training stage to the development stage throughout their careers, adapt processes with teaching patterns changes at schools or in distance teaching; on the inter-ministry level, it is recommended that the Ministry improve its partnerships with other bodies at the National Child Online Protection Bureau and apply the insights of the National Bureau's insights.

Abstract | **Part two - Ministry of Education actions to prevent harm to students on the online space**