FARO

Frontline Aggregated Record of Online Harms

FIELD REPORT #1: TECHNOLOGY IN EDUCATION

Shield.

FARO Field Report #1: Technology in Education

Frontline Aggregated Record of Online Harms · October 2026

AUTHOR

Angeline Corvaglia
Executive Director, SHIELD – APS

PUBLISHED BY

SHIELD – APS (Associazione di Promozione Sociale), Lecce, Italy
Fiscal Code: 93174300751
shieldthefuture.com · contact@shieldthefuture.com

FUNDING

This report was made possible with funding from NetHope through its Connected AI Grants. The findings, interpretations and conclusions are those of the author and do not necessarily reflect the views of NetHope.

SUGGESTED CITATION

Corvaglia, A. (2026). *FARO Field Report #1: Technology in Education.* SHIELD – APS.

DATA AND PRIVACY

Records reviewed up to 19 October 2026. Names and details that could identify a person or a school have been removed. The incidents behind this report can be viewed in the FARO incident directory: shieldthefuture.com/faro-incident-directory

© 2026 SHIELD – APS. All rights reserved.

TABLE OF CONTENTS

01	Executive Summary	2
	Acknowledgments & Partnerships	4
02	Framing of the report	5
03	Report Status and Scope	8
04	Harm Patterns Found Across Multiple Countries	9
05	Different Responses to Harms	16
06	Other Findings	29
07	What Linking the Records Shows	33
08	Recommendations	36
09	Call to Action	38
	Annex 1: Reach, Additional Considerations and Methodology	39
	Annex 2: Useful Links	43

01

Executive Summary

FARO (Frontline Aggregated Record of Online Harms) is an incident reporting and analysis system. It collects accounts of how technology harms people in everyday life and links them across sources and countries, so families, regulators, authorities, and grassroots organizations can learn from cases outside their own school or country, beyond the few widely reported cases. This first report covers what happened to students, families, and school staff when school technology became part of learning. It draws on 266 incidents from 47 countries, including accounts told directly to SHIELD and its partners.

266
INCIDENTS

47
COUNTRIES

The same harms appear in several countries, despite different laws, school systems, and cultural realities. These are analyzed from three different perspectives: cross-country harm patterns, differing reactions to similar harms, and other small but significant findings. The harm patterns section explores harms arising from products' ability to access the open internet, the lack of proper consent, the inability to opt out of required technology, punishment for not using it, chats and images used to expose or hurt students and teachers, and technology that puts education behind a financial barrier.

The next section examines how schools, regulators, courts, and families handled similar harms in different ways. Responses to the same harm varied greatly, and what the harmed person or their family was left with depended on who received their report.

Responses to the same harm varied greatly, and what the harmed person or their family was left with depended on who received their report.

The third section presents a series of smaller findings included as warnings of decisions that can lead to unintentional harms. These are teachers running classes through everyday public apps, schools acting on monitoring alerts before anyone speaks to the

student, schools relying on a filter without sufficiently ensuring that it works, school registers that open with a teacher's password alone, schools requiring screen time with no paper alternative, and companies selling courses on loans that keep running after the course has stopped.

The main recommendation from this analysis is to publish findings about school products as fully as possible and make them easy to look up, so a school, regulator, or family facing harm can see what has already been found and done elsewhere. This is supported by regular collection and analysis, such as this one, of what happens to students, families, and staff once a digital product is in use, especially given the fact that local incidents are not regularly published by media, regulators, or courts. In addition, digital products used in an educational setting should be subject to regular, independent testing.

Acknowledgments & Partnerships

SHIELD – APS expresses its deep gratitude to the collaborating organizations whose expertise, local reach, and financial support made this report possible:

FUNDING PARTNER

NetHope (through its Connected AI Grants)

RESEARCH & TAXONOMY PARTNER

Internet Safety Labs

LOCAL DATA & INSIGHTS PARTNERS

Digital Wellness Africa

Internet Safe Kids Africa

Eveminet Communications Solutions Limited

Social & Media Matters

We extend our sincere thanks to these organizations for their leadership, data collection efforts, and commitment to mapping and mitigating digital harms in education.

02

Framing of the report

Improvements in product safety tend to follow a chain. A harm happens, someone notices, someone reacts, it gets recorded, research or a ruling assesses it, individual actions are taken to prevent it from continuing, safety standards are eventually created around those experiences, and those standards eventually shape what happens going forward. This is a long, complicated process that relies on a clear understanding of what harms are happening and to whom, but unfortunately, those early elements of the chain have a structural gap in regular, widespread information. In the case of digital product safety, which is the area in which this report would fall, that pattern has not even been solidified yet. FARO was created to help fill that gap. It uses qualitative data triangulation, drawing on a wide range of sources: news reports, court cases, regulatory decisions, research, incident databases, people's own posts, and personal accounts.

FARO was created to help fill the digital harms information gap.

Although FARO reports will, in some cases, explore relatively unknown areas, significant work has already been done to explore the impacts of technology in education. A number of organizations are already working to help build a culture of assessing the safety of technology used in educational settings. Four pieces of work have served as an important basis for the understanding and analysis here: the 2022 report "How Dare They Peep into My Private Life?" by Human Rights Watch, the "2022 US K-12 EdTech Benchmark" by Internet Safety Labs, the 2026 "EdTech for Good Framework – Version 2.0" by UNICEF, and the 2026 policy brief "How Prepared are African Education Systems for Classroom Content Risks?" by Africa Program Real Life Research Institute. Links to these pieces of work can be found in Annex 2, page 45. Some of the key points about them are:

- **Human Rights Watch** reviewed 163 education products endorsed by 49 governments during Covid-19 school closures. They found that 145 appeared to use children's data in ways that put their rights at risk, contributed

to undermining them, or actively infringed on them.

- **Internet Safety Labs** tested 1,357 apps recommended or required by 663 randomly sampled US schools. 96 percent of them were deemed unsafe for students due to sharing children's personal information with risky third parties. It also found that 28% of apps were not specifically made for education and therefore did not provide the specific protections necessary for the children who use them, and that 23% of school apps exposed kids to digital ads, more than half of which used retargeting ads.
- **UNICEF**'s framework was developed together with the Finnish Ministry for Foreign Affairs, the Asian Development Bank and Arm, drawing on feedback from over 140 organizations in more than 60 countries. It is designed to support decision-makers in assessing whether a product is designed for good and with clarity, responsibility, and accountability. It has been used to assess over 1,000 EdTech tools.
- **Africa Program Real Life Research Institute**'s policy brief assesses how prepared African educational systems are to manage content risks, with a focus on Cameroonian, Kenyan, and Zimbabwean perspectives. It found a persistent gap between legal commitments on children's digital rights and what happens in classrooms. Although foundational laws exist, schools often lack enforceable rules on consent, recording, takedown, and reporting.

This report complements those four pieces of work by providing additional evidence of what happened to people using the same or similar products over several years and across different cultural and economic realities.

The largest single group of harms in the collection campaign for this report concerns required learning products collecting and sharing children's data. Because Human Rights Watch and Internet Safety Labs have already documented this extensively, this report does not repeat it as a pattern of its own.

It is also crucial to note the geographical limitation of what information the collection campaign was able to unearth. Although technology is used in education in varying degrees around the globe, reporting on its impacts is disproportionately focused on a few wealthy countries. A massive information gap exists for Global Majority countries. The majority of incidents from these countries that are referenced appear thanks to the Human Rights Watch study, and mostly describe products that governments endorsed during Covid-19 school closures.

Important Definitions

In this report, an incident is the recorded account of something that happened, or of something documented about a product in use, in connection with technology in education. Most incidents describe what happened to a student, a family or a member of school staff. Some describe a finding, such as a regulator's decision, a survey or an audit, where no single person is named.

In the understanding used here, technology in education covers two situations. The first is technology used directly during the learning process, such as products a school, ministry or teacher supplies, requires or chooses for teaching, learning or running a school. The second is when an educational setting brings about shared technology use among people who otherwise would not naturally be in a shared group online, such as a class WhatsApp chat.

The latter includes cases where the technology is a public platform the school did not choose but had implications for an individual or group's ability to thrive in an educational setting, such as Deepfake images of classmates shared on social media. The report calls technology that schools supply or require products, and uses app for a public app that a class is run through.

03

Report Status and Scope

This report is a proof of concept. It shows how collecting accounts of harm across borders reveals patterns that single schools, regulators, and countries cannot see on their own. It is currently designed to map how harms happen, not to be used as a measure of how often they occur.

FARO currently designed to map how harms happen, not to be used as a measure of how often they occur.

Because this is an initial study built with limited resources, readers should keep two points in mind:

- **Unequal coverage across countries:** Almost half of the incidents come from four countries: the United States, Italy, India and Zimbabwe. In many Global Majority countries, incidents are documented only irregularly or by one body that regularly publishes its activities, such as the court system or regulators.
- **Early-stage collection:** Many of the findings are based on a small number of incidents. They successfully show that a specific issue exists across communities and can happen elsewhere, but this report does not claim to show its full scale.

As FARO grows and adds local partners, future reports will draw on broader, more balanced records.

The following sections move on to the findings: harms that occurred across countries, how they were handled, and what emerges when incidents from different locations are compared.

04

Harm Patterns Found Across Multiple Countries

Despite different laws, school systems, cultural and economic realities, and digital products, technology in ordinary use produced similar harms across diverse communities. Each pattern below describes the problem, followed by some cases from the records. Annex 2 links to the full list of cases. Patterns that are included in this section were reported across at least 3 different countries with a minimum of five separate similar incidents.

Pattern 1: Inappropriate content gets in

52	18
INCIDENTS	COUNTRIES

In 52 incidents across 18 countries, harms were observed that were made possible because the product used for education was connected to the open internet without effective enough filtering. This allows the school's own product to be used in ways it was not intended, such as becoming a route to pornography, violent content, and adult strangers. In the records from this FARO campaign, children accessed this kind of content in class, at recess, and at home on school-issued devices. In 14 of these incidents, across 5 countries, the material was shown to a whole class through a classroom screen, a projector or an online lesson, from an adult's or a visitor's own computer or through a shared link to a lesson.

If devices used for educational purposes are connected to the open internet, filters are usually the main security mechanism. Although filters narrow what gets through, they don’t always fully protect children from inappropriate and damaging content. These are a few of the incidents in the data set:

- In Sweden, lower-grade pupils viewed pornographic and horror content during class even though the school had an active content filter.

- In Indiana, in the United States, a parent discovered that her 7-year-old daughter had recorded videos of herself after being exposed to pornographic images and videos found via a YouTube search on her school-issued iPad.
- Multiple anonymous posts on a Japanese Q&A forum show students discussing access to pornographic content on school-issued iPads.
- In Scotland, in the United Kingdom, a primary school pupil was left traumatized and in shock after classmates searched for a medical term on their school laptops and explicit content came through the school's safety filter.
- In Spain, a parent told SHIELD that a six-year-old child viewed violent movie trailers through a platform used at school.
- In New Zealand, children accessed harmful, sexually explicit content on primary school iPads despite a NZ$33 million government investment specifically intended to fund school device safety systems.
- In Ghana, the Minister for Education publicly warned that some high school students were using government-issued tablets to reach pornographic content.
- In Quebec, Canada, a wrong file with explicit adult content opened on a police officer's laptop during a talk to Grade 10 students on sexual assault and consent, and was projected for a few seconds.
- In Italy, in three cases, intruders joined online lessons and a primary school's online open day through shared links and showed pornographic or violent videos.

Parents' posts in online forums also show children reaching this content at home and at recess, sometimes when the device is used away from the school network where effective filters are in place. In 8 of these incidents, across 7 countries, the school or ministry had a filter or block in place and it still failed.

Wherever a school product connects to the open internet, the school relies on filters to protect children, and these incidents show that filters alone do not offer sufficient protection.

→ See the incidents behind this pattern in the FARO directory: Pattern 1: Inappropriate content gets in

Pattern 2: Required tech, no opt out

110	36
INCIDENTS	COUNTRIES

This pattern involves technology that was implemented on a mandatory basis without proper consent or the ability to opt out. It was found in 110 incidents across 36 countries. There are two types of cases: products chosen by schools or districts, and products endorsed by governments. In many of these cases, the required learning products tracked children's location at home, collected their contacts, passed their data to other companies, and put their real names, faces, or even actions on public video profiles. In many cases, families had little room to refuse without consequences for their child's schooling. The pattern also includes cases where students or staff were punished for not using a required product.

- In Denmark, a public school required students to use school-provided laptops and set up public profiles on a video-sharing platform. This exposed a student's personal details, including their full name, age, school name, and class, without parental consent.
- In the United States, a parent and her children had their sensitive educational, medical, and behavioral data collected, tracked, and commercialized without parental consent through mandatory school software. The data was allegedly sold to over 100 third-party commercial partners to predict and profit from the children’s future trajectories.
- Human Rights Watch found that millions of students were effectively forced to choose between being surveilled and being educated. In most cases, children could not opt out of data collection without giving up access to compulsory schooling during the pandemic. For example:
  - In Turkey, a 9-year-old boy required to use online learning platforms to attend class had his location at home tracked and his family's and friends' contact details downloaded, without his or his mother's knowledge.
  - In Iran, students required to use the government's learning app had their precise location, contacts, and contact photos collected without being told.
  - In India, the required Diksha learning application collected a student's precise location, timestamps, and device identifiers and shared the data with Google.

- In Kenya, a parent told Eveminet Communication Solutions that a school app required identity numbers, phone numbers, and payment details without a clear privacy policy or information on what would be done with the data.
- In the United States, a parent told SHIELD that the family could not opt out of the school's digital systems without consequences for the child's education.

When a school or a government makes a product mandatory, it makes decisions about the child's data on the family's behalf, and in these incidents, families only found out what those decisions involved after the fact.

Students and staff were also punished for not using a required product, sometimes even when they had no control over it.

- In Ireland, a girl's required tablet was away with the vendor for repair, and her school repeatedly gave her demerits and detentions for not having it.
- In the United Kingdom, a boy was given detentions for not logging his reading through a required app that limited book choice, controlled reading speed and set AI-generated quizzes.
- Human Rights Watch found that in Iran, school administrators told a teacher they would be marked absent if they did not install and use the government's education app.
- In Italy, a teacher was given a 1-day suspension for keeping a paper record, even though the school had not given the teacher a device.
- One Reddit user also said that after their school heavily pushed generative AI tools on students, they openly expressed opposition to using them. Educators and school administration began to exclude and subtly mistreat them until they withdrew.
- Two teachers on Reddit described being made to install a school app on their own phones. One faced backlash from administrators after questioning it, and the other had to hand the phone to the vice principal to have the app installed.

When a digital product is the only way to do schoolwork or to teach, not using it is sometimes treated as not taking part in school or not doing the job rather than something unrelated, such as when the product is broken, missing, or something they object to.

→ See the incidents behind this pattern in the FARO directory: Pattern 2: Required tech, no opt-out

Pattern 3: Weaponization of chats and images

35	12
INCIDENTS	COUNTRIES

In 35 incidents across 12 countries, chats and images connected to a school were used to share sexual or violent content, or to expose, mock or threaten a classmate or a teacher. This covers class and school group chats, and images or videos of students and teachers that others created or shared, including AI-generated images. In the records, the person harmed was often a child, and the content sometimes reached the wider public.

- In Italy, a class chat at a secondary school was used to post pornographic videos, extremist content and insulting videos of teachers.
- In Italy, manipulated nude images of two 14-year-old schoolgirls were created with an app and circulated among schoolmates.
- In Zimbabwe, a high school student had intimate photographs shared to a school WhatsApp group by a former boyfriend, and she experienced severe fear and stopped attending school.
- In Kenya, a 21-year-old university student endorsed a candidate in her class WhatsApp group during a student election and was then harassed for weeks with vulgar comments about her body. She withdrew from school and student activities.
- In Nigeria, a university student's private video was leaked online without her consent in 2019, and her university expelled her.
- In Spain, the juvenile prosecutor opened an investigation into three minors at a school accused of using AI applications to generate sexualized images and videos of 61 people, including 22 minors and several teachers, and sharing them among students.
- In the Netherlands, a national news outlet surveyed about 400 primary schools and found that several reported pornographic and extremely violent video material shared in class-wide chat groups.

In four of these incidents the person whose private video or assault was circulated was then suspended or expelled by the school.

→ See the incidents behind this pattern in the FARO directory: Pattern 3: Weaponization of chats and images

Pattern 4: Paid access to schoolwork

13	7
INCIDENTS	COUNTRIES

In 13 cases across 7 countries, required schoolwork could only be done on a product that families and school staff had been required to pay for themselves, effectively creating a barrier to education. In some cases, students whose families could not pay lost access to the schoolwork itself, and in others families and staff took on finance deals or pay cuts to keep their place. The cost reached people in three ways. Schools required families to pay for or supply a device, an education board required teachers to buy their own, and a government charged for access to learning content.

- In Spain, a school restricted students' access to individual tablets, laptops, and the required digital educational platform if their families did not pay an annual ICT fee. As a result, affected students were forced to share devices and rely on physical paper agendas, which lacked the exclusive communication and schoolwork content uploaded to the digital platform.
- In Northwest England, a mother on a low income was told she must pay £600 or sign a three-year finance agreement for the tablet her child's new secondary school required, and the school refused to offer a free alternative.
- In Nigeria, a state education board issued a directive forcing secondary school teachers and non-teaching staff to acquire ICT tablets. The educators were required to purchase the devices out of pocket or enroll in a salary-deduction scheme with a private vendor, and their employer warned that failure to comply would disqualify them from career promotions.

- Human Rights Watch found that in Zambia, students were encouraged to use educational platforms where access to some educational content and exam preparation materials required payment or subscription fees.
- In Italy, parents were given a circular saying that students without an iPad should continue their studies at another school, with devices required from third grade of primary and first year of lower secondary.
- In Texas, in the United States, a college student spent forty dollars on a second phone because the required login app would not run on the phone they had.
- In the United Kingdom, a family paid over £1,000 for a required device that often malfunctioned, and the school later dropped the scheme and went back to books.
- In Ireland, parents posting in one online thread described the cost of the mandatory school device. One was quoted €640 on a 12-month plan, and the payment plan raised the total to €786.99 over 36 months. Another said a device costing nearly €1,000 stopped working before the first school year ended and no refund was given.

When schooling can only be done on a paid product, the cost of taking part in school moves to families and staff, and those who cannot pay lose access.

→ See the incidents behind this pattern in the FARO directory: Pattern 4: Paid access to schoolwork

The patterns above show harms that repeated across countries. The next section shows what came after them, arranged by stages of the risks cycle. It covers responses from schools, regulators, courts, police, and families, including cases where the response fell on the person who was harmed.

05

Different Responses to Harms

The same harm can have very different long-term consequences depending on who responds to it and how. This section highlights different reactions to similar harms across a variety of countries, and among different actors within the same country.

The responses below are arranged by stages of the harms and risks cycle that they belong to.

MEASUREMENT | AWARENESS | PREVENTION | MITIGATION | ACCOUNTABILITY | OUTSIDE THE CYCLE

Measurement means finding out how much happened. Awareness means telling people. Prevention means changing things so it does not happen again. Mitigation means reducing the harm now. Accountability means answers and consequences. A sixth group, Outside the cycle, contains responses that left the product in use or fell on the person harmed. Each section shows only the stages with relevant records for that topic.

Accountability is the largest group, with responses such as fines, reprimands, investigations and lawsuits. Measurement and Awareness each appear only once across the five sections. This analysis is done based on what the records make visible and it not intended as an exhaustive collection of how these harms were responded to. It also does not assess what schools and authorities do well, or how often any response happens. A response that leaves a public trail, such as a regulator's decision or a court case, is more likely to be recorded than a quiet change to a setting or a conversation with a family.

Responses: Inappropriate content gets in

Children reached pornography on tablets, laptops and computers their school supplied, in class, at recess and at home. Responses ranged from a national withdrawal of tablets to keeping a device in use after a parent showed that its filter could be bypassed.

MEASUREMENT

Looked for other affected children.

California, United States, 2019.

A mother found her second-grader had watched adult pornography on her school tablet. The district reviewed browsing histories on tablets across five elementary schools and found that several other children in the same class had also reached inappropriate content.

PREVENTION

Reviewed device security settings.

Illinois, United States.

Students across a school district were found to have reached pornography on school tablets. The district responded by reviewing the security settings on its devices.

Gave officers dedicated laptops.

Canada, 2025.

During a police talk to Grade 10 students on sexual assault and consent, a wrong file with explicit adult content opened on the officer's laptop and was projected for a few seconds. The school board told parents and offered support to students, and the police said officers would get dedicated, pre-configured laptops.

Reviewed the rules on staff devices.

United States, 2022.

An employee plugged a personal laptop into a classroom projector and explicit images from an online image search appeared. The employee was placed on leave, students were offered counseling, and the district reviewed its policy on personal devices in classrooms.

MITIGATION

Withdrew all primary school tablets nationally.

Andorra, 2026.

After pupils reached sexual content on classroom tablets despite safe search being in place, the Ministry of Education withdrew the tablets and committed to a full security audit with the search company and the national telecom provider before returning any.

Blocked the site or fixed the filter.

Singapore, Wisconsin and Norway.

In Singapore, in March 2026, a father found that his two secondary school children could reach videos bordering on soft pornography through a video site on their school learning devices, despite the controls installed. He reported it to the Ministry of Education, which blocked the site within days and offered to meet him. In Wisconsin, United States, in 2021, a mother found her 5-year-old had reached a pornography website on a school laptop at home. The district confirmed the filter had not worked off the school network for about two months. It said it fixed the gap within hours of finding it, but it did not tell all affected families, and it disputed parts of the mother's account. In Norway (account given to SHIELD), a parent found that children in their child's elementary class were sharing links to pornography on school tablets two weeks after the tablets arrived, and told the school, the district, the media and the government. Filters were put in place at once. Government guidance on filtering school devices arrived a year and a half later.

Offered trauma support.

Norway.

After books were replaced with internet-connected tablets, children began showing each other pornography in class. The school offered the children trauma counseling.

Removed the group.

Italy, 2026.

Activists invited to give a talk on animal welfare connected their own computers in a primary classroom and projected footage of industrial slaughterhouses. Many children cried, and teachers removed the group from the building. The head teacher said the school had been deceived.

ACCOUNTABILITY

Looked for who was responsible.

India, 2025.

In Madhya Pradesh, a pornographic video was played on a classroom screen at a public school with about 13 children present and no teacher in the room, and a pupil's recording of it spread on social media. Local education officials set up a three-member committee to find out how it happened and who was responsible. In Himachal Pradesh, a student allegedly played an obscene clip during an online class at a government school. A mother complained to the school and alleges that no action followed and that her teenage

daughter was harassed at school afterward, so she went to the police. The school's disciplinary committee could not identify who was responsible, and the police cyber cell is investigating.

Reported the intruders to the police.

Italy, 2020 and 2021.

In three cases, intruders joined online lessons or a primary school's online open day through a shared link and showed pornographic or violent videos, and head teachers or class representatives reported them to the postal police. At a high school in Tuscany, the head teacher also warned parents that students who shared lesson links risked a criminal complaint. At a middle school, parents asked the head to tell all families what security standards the school used for online lessons.

Sued the device maker.

Utah, United States, 2026.

A family sued Google, alleging that their child's school-issued Chromebook failed to block and instead promoted pornography, and that the child developed an addiction. The claims have not been decided as of this report's publication.

OUTSIDE THE CYCLE

Did not believe it.

North Carolina, United States, 2024.

Older pupils on the school bus showed an 8-year-old how to reach an age-inappropriate game on his school laptop, and his mother then found he could also reach sexually explicit images. A school technology administrator told her this was impossible. She showed the vice principal, and the principal replied that the boy had to keep using the laptop so he would not fall behind. According to the mother, the district conceded its filter does not reliably work.

Dismissed the child's report.

Florida, United States, 2015.

Older pupils repeatedly showed an 11-year-old special education pupil pornography on a school tablet at recess for about three months, and threatened him not to tell. When he reported it, a staff member reacted dismissively. The family sued the school district.

Did not answer questions.

Indiana, United States, 2020.

The district did not answer specific questions about the case. The mother withdrew her children and went public to warn other parents.

Said it was the head teachers' job.

Italy, 2016.

Pupils aged 7 and 8 reached pornographic sites on unfiltered computers in a primary school lab during a supervised lesson, while the teacher believed blocking was active. A parents' group said it would ask the Ministry for a check of school IT security, and the Ministry said that choosing, installing and maintaining the systems was up to head teachers.

Where a district looked beyond the one report, it found more. In California, reviewing browsing histories across five elementary schools found several other children in the same class who had reached inappropriate content, and in Wisconsin the district confirmed that the filter had not worked away from the school network for about two months.

→ See the incidents mentioned in these responses in the FARO directory: Responses when inappropriate content gets in

Responses: Required tech, no opt-out

Learning platforms, accounts, and devices that schools or governments required collected children's location, contacts, messages, photos, and activity. They passed these to advertising and other companies without families being told. The responses recorded range from a ban on the products to fines on schools and lawsuits brought by families against the companies. Some responses concern students and staff who were punished for not using a required product.

MITIGATION

Banned the products and ordered the data deleted.

Denmark, 2022, and Norway, 2020.

In Denmark, the data protection authority upheld a ban on a municipality using its school laptops and accounts for pupil and teacher data, because the risks of the provider processing that data had not been dealt with. Pupils and teachers began the 2022/2023 school year without their main digital teaching products. In Norway, a municipality used a school survey in which classmates named pupils as bullies, victims or disruptors. There was no legal basis for it, and named pupils could not see or correct what was said about them. The data protection authority and the appeals board ruled it unlawful and ordered all the data deleted.

Withdrew her children.

California, United States, 2025.

A mother whose children were required to use a learning platform that shared their data with other companies without her consent withdrew them from the school district.

ACCOUNTABILITY

Issued an injunction and an order.

Denmark, 2024, and United States, 2023.

In Denmark, a parent campaigned until the data protection authority issued an injunction against schools using the platform for pupil data. In the United States, the Federal Trade Commission's complaint said a learning platform collected names, contact details, dates of birth and identifiers from children under 13 without parental consent, used them for advertising and kept them indefinitely. The order sets a schedule for keeping and deleting data and carries a $6 million penalty, suspended because the company could not pay. The company had stopped operating in the United States during the investigation, and the order applies if it returns.

Fined or warned schools, municipalities and a university.

Spain, Norway and Italy.

In Spain, in 2026, after a parent complained, the data protection agency fined a school €20,000, later reducing it to €12,000. The school had set up a learning suite for more than 500 pupils, including children under 14, without informing families, obtaining lawful consent or assessing the risks of sending their data abroad. In Norway, pupils at two

schools were told to use a fitness tracking app for school activities, and the municipality lost control of how their data was used.

The data protection authority fined it 50,000 kroner. In Norway, in 2020, the authority warned three municipalities that it would reprimand them for rolling out school laptops and accounts without assessing the risks, without a proper legal basis, and without telling pupils and parents how their data would be used. In Italy, in 2024, a university made students consent to periodic face scans, matched against their ID, as a condition of taking an online teacher training course. The data protection authority fined it €50,000 for unlawfully processing their biometric data.

Went to court.

United States.

Analytics and advertising software built into a school platform intercepted pupils' confidential messages, and in 2026 a class action ended in a $17.25 million court-supervised settlement. In 2025, pupils and parents sued a learning company for tracking pupils during school-required use, and a federal judge refused the company's request to move the dispute into private arbitration, ruling that schools cannot bind families to such terms. In Washington State, in 2026, a federal judge ruled that a mother's privacy claims against the company behind the required school software could proceed. In 2025 and 2026, pupils filed class actions against Google, Seesaw, Renaissance Learning and Curriculum Associates, alleging that their products collected and shared pupils' data without consent. These claims have not been decided as of this report's publication.

Annulled the teacher's suspension.

Italy, 2018.

The teacher suspended for keeping a paper register appealed with a lawyer from a teachers' union. A labor court annulled the sanction, finding no proof she had a device to fill in the register, and noted that teachers received tablets only after the disciplinary charge.

OUTSIDE THE CYCLE

Gave detentions.

United Kingdom and Ireland.

The UK school gave detentions to the boy who would not log his reading in the required app. The Irish school gave the girl demerits and detentions while her iPad was with the vendor, and the vendor fixed it only after her parent complained to its

chief executive and posted about it on LinkedIn.

> Requiring the product removed the option of saying no. A family, pupil or teacher who objected could not simply decline and carry on at school. Refusing or failing to use the product was treated as a problem with the person, and it brought discipline, suspension or leaving the school. The school or municipality that made the requirement faced consequences only when a parent, a union or an authority raised it later. The choice to require the product was made once, by the institution. The cost of it was carried by the people who had no part in the choice.

→ See the incidents mentioned in these responses in the FARO directory: Responses required tech no opt out

Responses: Private details exposed

School registers, email, communication platforms and login systems showed pupils' psychological evaluations, disability and health details, education plans and national identity numbers to classmates, other families and companies who should not have seen them. The responses recorded range from regulators' fines and reprimands to institutions reporting their own errors and one school asking its software supplier for a change.

PREVENTION

Asked the software supplier to add a warning.

Italy, 2025.

A school sent a vaccination reminder to about 37 families with every address visible, which showed whose paperwork was missing. The school reported the breach, retrained staff and asked the company that supplies its email program to warn users when several recipients are entered. The data protection authority fined it €1,000.

MITIGATION

Had the image taken down.

Spain, 2020.

A regional school management system printed five pupils' national identity numbers on student council ballots, and another pupil posted a photo of the ballots on Instagram, where about 250 people saw it. The school worked with the platform to have it removed.

ACCOUNTABILITY

Reprimanded five municipalities.

Denmark, 2024.

A school communication platform sent pupils' psychological evaluations and dyslexia reports to the wrong recipients. The data protection authority found the municipalities had not assessed the risks properly, reprimanded all five, and ordered two of them to complete a data protection impact assessment within three months.

Fined, reprimanded or warned schools.

Italy, 2024 to 2026.

A school sent meeting schedules through its register that included the initials of 52 pupils with disabilities, so other parents, teachers and pupils could recognize them, and the data protection authority fined the school €1,000. A support teacher uploaded a pupil's education plan to the register with settings that showed it to every parent in the class for about 22 minutes. Another parent took a screenshot and shared it in a class messaging group. After the family complained, the authority reprimanded the school. In five more cases, a school register sent a pupil's Covid-19 test result, education plan, disability details or private evaluation to classmates and their families. The authority warned, admonished or fined each school.

Reported the error to the regulator.

Norway, 2024.

An error in the national education login portal sent the national identity numbers of 15,019 students and staff at a university to outside learning providers when they logged in, and 7,873 of them had their data stored by those providers without prior agreement. The university reported it to the data protection authority.

Nearly all of these responses were addressed to the school or municipality that sent the details. Only in one Italian region was the tool itself addressed, when the school asked its email supplier to warn users when several recipients are entered.

→ See the incidents mentioned in these responses in the FARO directory: Responses private details exposed

Responses: Weaponization of chats and images

Chats and images connected to school were used to share sexual or violent content and to expose or mock classmates and teachers. Responses came from schools, police, prosecutors and courts. Some acted on the content, some focused on the people who made or shared it, and in several cases the school's response fell on the person whose image or video had been shared.

MITIGATION

Ordered the content deleted.

Italy.

After a pupil forwarded a child sexual abuse video from a game chat into a middle school class chat, the judicial authority ordered the content deleted from all the phones of the children involved and the devices restored to factory settings.

Shut down the group.

Italy.

Authorities shut down a group of hundreds of middle school students in two municipalities that had been circulating pornographic images, and schools and community organizations promoted awareness initiatives.

AWARENESS

Ran a prevention campaign.

Germany, 2021.

The state criminal police launched a statewide campaign on illegal and harmful content on students' smartphones, after police saw pornography and violence videos being shared by children in student chat groups.

ACCOUNTABILITY

Reported and suspended the students.

Italy.

Six students were reported and suspended after a class chat was used to post pornographic videos, extremist content and insulting videos of teachers.

Opened investigations and made arrests.

Italy, Spain, Switzerland, Nigeria, India and Zimbabwe.

In Italy, police seized phones and a juvenile inquiry was opened after manipulated nude images of two schoolgirls circulated among schoolmates. In Spain, the juvenile prosecutor opened an investigation into three minors accused of generating sexualized images of 61 people with AI applications. In Switzerland, a parent's report to the police led to an investigation involving an entire class, and authorities confiscated phones. Police in Nigeria arrested and arraigned six students on charges of cyberstalking and assault after a recorded assault on a university student circulated online. In India, two college students were arrested and charged under the POCSO Act after allegedly morphing and circulating obscene images and videos of teachers and female students. In Zimbabwe, a government investigation and possible criminal proceedings followed a video of teachers allegedly assaulting a student on a school bus. After a video of a 16-year-old student with his teacher leaked and spread on social media, a child-protection investigation began and the teacher was arrested.

OUTSIDE THE CYCLE

Said it was outside the school's control.

Italy.

After a pupil shared a video of a sheep being slaughtered in a class chat, the headteacher said the chat was private and on students' own phones, and so not directly within the school's control. The school discussed the incident with students and included it in citizenship education, while parents consulted a lawyer.

Expelled the person harmed.

Zimbabwe.

After a video of the sexual assault of a 17-year-old student with learning difficulties went viral, the school expelled her together with the two schoolmates who had assaulted and recorded her.

Suspended a ten-year-old and allegedly threatened her.

Nigeria, 2022.

After a video of the girl being coerced into a sexual act by classmates on a school trip circulated on social media, the school suspended her and allegedly threatened her to stop her speaking out.

Expelled or suspended a student after a private video leaked.

Nigeria.

In 2019, a university expelled a student after her private video leaked, which prompted widespread criticism that it shifted blame to her. In another case, after a private intimate video of a student union president was leaked and shared on social media, the university suspended the president and opened an investigation to find who had leaked it. A national student association disputed the suspension as a violation of the student's privacy rights.

Many of these responses came from police, prosecutors and courts. In Italy, a judicial authority ordered the content deleted from the children's phones. In Zimbabwe and Nigeria, schools suspended or expelled the person whose video had been shared.

→ See the incidents mentioned in these responses in the FARO directory: Responses weaponization of chats and images

Responses: Paid access to schoolwork

When a school product is required, a pupil, family or teacher who cannot pay for it, cannot use it or does not have it can lose access to schoolwork or be penalized. What happens next depends on who responds. In these records, schools generally kept the requirement, and in one case an outside body stepped in.

ACCOUNTABILITY

Opened an investigation into the school.

Spain, 2025.

After families complained that pupils had lost access to devices and the learning platform over an unpaid fee, the regional education authority opened an investigation into the school.

OUTSIDE THE CYCLE

Refused a free alternative.

North West England, United Kingdom.

The school kept the £600 requirement after the mother explained she was on a low income.

Told families to move school.

Italy, 2022.

The head teacher defended the letter to parents in their school community telling families without an iPad to continue at another school, and said the school lends devices to some families.

Offered a move to another class.

Italy, 2016.

Families at a high school were told two weeks before the end of term that staying in the digital class section meant buying an iPad for about €600, on top of €300 to €400 for books. The school head said families could move to the traditional section or change schools.

In all three school responses, the requirement stayed. The family's options were to pay, or to leave the digital class or the school. The one response that put the requirement itself under review came from a regional education authority.

→ See the incidents mentioned in these responses in the FARO directory: Responses paid access to schoolwork

In most of these cases, nothing happened until the person harmed or their family raised the problem, and what followed depended on who received it. In these records, the same harm ended very differently from one school or country to the next. The exceptions were where a regulator checked schools on its own initiative, as in Denmark, or an institution reported its own error, as in Norway.

The next section returns to patterns, focusing on smaller patterns that do not have the same cross-country spread as the previously presented harm patterns but which can still be valuable to watch for, as some of the key factors allowing harms are small choices.

06

Other Findings

These findings are included here as warnings about behaviors that can lead to unintentional harms. Each comes from a choice made by a teacher, a school, a district or a company. Each item below says which countries its records come from.

Classes run through everyday public apps

Some teachers and schools chose to run class communication, homework or school activities through public apps. When they do, the app's age rules, features added after it had already been assessed and mandated, and open access come with it. The school has no way to switch them off.

- In Italy, a parent told SHIELD that a teacher required class messages to go through a messaging app. When the app added an AI chatbot, the parent had no way to keep the child from it while the child still took part in class communication. The school chose the app, but the company decides what to add later, and the class gets that too.
- Human Rights Watch found that in Turkey, a teacher required a 9-year-old to open a social media account to hand in homework, despite the platform's age limit. The homework requirement put a child on a platform below its own minimum age.
- In Norway, pupils were told to use a fitness tracking app for school activities, and the municipality lost control of how their data was used. Once pupils' data is in a commercial app, the school no longer decides what happens to it
- In India, an outsider got into a school's online classes and messaging groups, targeted nine schoolgirls and five female teachers with harassing calls and messages, and circulated morphed nude and semi-nude photos of the students. The same access that lets the class meet online also lets a stranger reach the pupils.

→ See the incidents behind this finding in the FARO directory: Classes run through everyday public apps

A software flag on a student's own work brings adults in

Some schools and districts chose monitoring software that reads students' documents, artwork, searches and behavior, and decided to act on its flags before anyone talked to the student.

- In a California district, students flagged while doing homework research or playing games were questioned by police instead of by staff. They said they felt traumatized, criminalized, and distrustful of school staff. The alert went to the police before anyone at school asked students for the full story.
- In Washington state, adults read a student's private writing about suicide after the software flagged it, and the student said the embarrassment lasted for years.
- In Kansas, the software falsely flagged student artwork as child pornography and let administrators read unpublished student journalism, and the students sued.

→ See the incidents behind this finding in the FARO directory: A software flag on a student's own work brings adults in

Students change grades with a teacher's password

In multiple cases in Italy, the electronic register that keeps track of grades, absences, and entry times was successfully opened by one or more pupils, so those who got hold of it could change the record, sometimes for many classmates. This happened at five schools.

- At one middle school, pupils used the passwords of at least four teachers for at least 40 accesses, turning failing grades into top marks and giving strong classmates very low ones, and it came to light only when a teacher noticed one odd low grade.
- At an upper secondary school, one password spread through student chats and about 40 students changed their entry times and absence notes.

Where a response is recorded, it was aimed at the students, through disciplinary sanctions, police reports and court cases rather than at the system that made the breach possible.

→ See the incidents behind this finding in the FARO directory: Students change grades with a teacher's password

The course loan outlives the course

Some online learning companies in India sell courses on loans arranged by the company or its lending partner, and families who want the best for their children choose to utilize the offer. However, when the course was canceled or stopped, the loan kept running.

- A relative who canceled a three-year course for a 12-year-old within the promised 15-day window got back only part of what he paid
- A father in West Bengal kept seeing monthly deductions after canceling, until a consumer commission ordered a refund and compensation.

When another company stopped its classes, parents kept paying their loans, threatened with damage to their credit score and visits from recovery agents. Because the loan is a separate agreement with a lender, canceling the course does not cancel the debt, and the family keeps paying for teaching the child no longer gets.

→ See the incidents behind this finding in the FARO directory: The course loan outlives the course

Required screen time

Some schools make daily device use or online-only homework part of schooling. When a family wants to reduce screen time, the schoolwork can leave no way to do it.

- In the United Kingdom, a parent removed all digital devices from her daughter because of concerns for her mental health. The school, which runs a fully digital curriculum, refused paper homework, and she could not complete her schoolwork.
- In the United States, a student had daily headaches after a school year of using and carrying a school-issued laptop, and her parent opted her out of the school's computer and digital curricula for the next year.
- In Pennsylvania, United States, a high school senior struggled to concentrate and her grades fell after daily school laptop use since kindergarten. Her mother asked the district to confiscate the laptop, and the district refused because the devices are part of the curriculum.

- In Italy, students reported in repeated surveys on a student portal that homework kept arriving through the electronic register, email or chat after school hours. In September 2026 the Ministry of Education sent schools a note ruling out register entries in the late afternoon, evening or at weekends.

→ See the incidents behind this finding in the FARO directory: Required screen time

The last three sections examined each case where it happened: what went wrong, how it was handled, and the smaller choices behind it. Many of the same products and harms appeared in more than one of those places. The next section looks at what that shows when the records are read together.

07

What Linking the Records Shows

Read together, the records often show each place finding the same problems for itself, usually through the person harmed, and the same company's products being acted on one country at a time. They also show that a response can start without a family coming forward, in the places where someone is checking.

Often each place finds a problem already encountered elsewhere

Many of the same school products are used in countries around the world, and the same problems come up again and again, but the majority of cases are handled by one school, district, regulator or court at a time. Furthermore, the person who discovers it is usually a parent, student, or teacher. In five US states, between 2015 and 2024, a parent found that a school device's filter had let a child reach pornography and took it to the school. In 2026, a father in Singapore and a teacher in Andorra found the same kind of failure on their own countries' school devices. In Italy, in 2020 and 2021, intruders entered online lessons and an online open day at several schools through shared links, and each school reported it to the police separately. In Norway, the school added filters as soon as a parent raised the problem, and national guidance on filtering school devices followed a year and a half later.

Because each place has to do the work of finding the problem again, each time the cost falls on the child who becomes a victim of the harm and the adult who has to help them through it. When a finding can be looked up by product and harm, the next school or ministry can check the products it chooses before harm occurs.

When each place that uses similar technology has to do the work of finding the harm, the cost falls on the child who becomes a victim and the adult who has to help them through it.

A product can only be understood when the incidents are looked at together

Individual products used globally, such as Google's school laptops and accounts, have been addressed separately in multiple countries, each time against a different party. In Norway, the data protection authority warned three municipalities in 2020. In Denmark, the data protection authority issued decisions against municipalities from 2021 to 2024, including a ban on one municipality's use of the products for pupil data. In Spain, the data protection agency fined a school in 2026. In the United States, families sued the company itself, over pupils' data and over children reaching pornography and strangers on school Chromebooks.

Each regulator acted at the municipal or school level, and each US case was brought by its own families. A fuller picture of what the product does to children appears only when these records are consolidated and viewed together. Findings about one product being findable across borders help a regulator or family in another country using the same devices build on what others have already established.

Where someone checks, proactive protection can help prevent harms

Internet Safety Labs found that only 14 percent of the US schools it sampled offered families a consent or opt-out form, and 29 percent had technology vetting in place. Human Rights Watch found that, during the Covid-19 pandemic, governments quickly endorsed or procured EdTech for schools in a rush to connect children to virtual classrooms, but few checked if it was safe. The Africa Program Real Life Research Institute found that schools in Cameroon, Kenya and Zimbabwe do not consistently have enforceable rules on consent, recording, takedown and reporting. UNICEF developed its framework in response to limited evidence available to decision-makers about which technology to introduce into school systems.

Ways to check a product before it reaches a child already exist: independent testing like that of Human Rights Watch and Internet Safety Labs, assessment frameworks like UNICEF's, regulators' audits, and institutions' own reviews of their systems. The sources this report draws on suggest these checks are not yet routine. Where these checks are used and their findings published, a school or regulator has something to act on before the next child meets the same risk. Reading them alongside regular collection of what happens once products are in use shows which of the risks found in testing have already harmed children, and where.

08

Recommendations

These recommendations are SHIELD's, drawn from the findings above. The first five are about how problems are found, checked and shared. The last three are about the harms themselves.

01 **Publish incidents and responses as fully as possible, by product.** Regulators and education ministries that decide a case about a school product should publish as much of the decision as the law allows: the product and version involved, what failed, what was required and by when, and which families were told. A decision that names the product can be found by a regulator or family in another country facing the same product.

02 **Check products in use without waiting for a complaint.** Data protection authorities and education authorities should mandate that manufacturers obtain independent audits of the digital products offered to schools. Internet Safety Lab's App Microscope is an example of what this could look like (https://appmicroscope.org/). UNICEF's framework also gives them a way to assess each product. Proactive reporting is also essential, even in the cases where the law does not specifically mandate it. Each audit and report should be published so other communities that need it can benefit.

03 **Look up what others have found, and file what was done.** A school or education authority facing a harm on a school-issued product should look into where else the product has been associated with harm and what the response was. Once it has acted, it should have a clear risk mitigation process in place: disclosing the incident, what the remedy was, and what the accountability is.

04 **Give families and staff a dedicated point of contact.** Schools and education authorities should name, for each required product, the person who receives reports about it. That person should give a written answer within a set time and, when a report is confirmed, check the other children's devices, as one California district did across five schools after a single mother's report.

05 **Fund regular collection where few decisions are published.** Governments, international bodies and funders that support or endorse school products should fund regular collection of accounts from pupils, families, teachers and local organizations. Governments already fund and staff incident reporting in other fields where products can harm people, such as aviation and medical devices, so that what goes wrong is collected in one place and can be compared across cases. School products need the same kind of incident tracking. This matters most where schools lack enforceable rules on reporting and regulators publish little, because what happens to children once a product is in use is known mainly through families.

06 **Build protection into the product.** Companies that make school devices and accounts should ensure they are safe and protect the privacy of children. The products themselves should be age-appropriate, and protections should not rely too heavily on filtering as the main layer of protection.

07 **Do not make schooling depend on the use of one or more digital products.** Whoever requires a digital product or app in an educational setting, whether a school, a state education board, or a ministry, should not pass its cost to pupils, families, or staff, and should keep an alternative that gives access to the same schoolwork.

08 **Tell families what a product does before it is used, and what happens if they say no.** Education authorities, including ministries that endorse or supply a product, should tell pupils, families and staff in plain language what each required product connects to, what it collects, what can be switched off, and what the alternative is for a family that refuses.

09

Call to Action

The more places and people it includes, the more useful FARO becomes. There are four ways to help make that happen.

Pupils, parents, teachers and school staff: tell FARO what you have seen with school products, especially if you live in a country where little public information is available. Accounts like yours are how those cases reach the record. *Submit an EdTech-related incident here: https://ee-eu.kobotoolbox.org/x/iaRJVLtE*

Schools, education authorities and regulators: before deciding how to respond to a harm, look up the product or the harm in FARO to see what others have found and done. *Search FARO incidents here: https://shieldthefuture.com/faro-incident-directory/*

Partner organizations: collect accounts with FARO in your country, so the record holds cases from communities like yours, including where regulators publish little. *Contact SHIELD: https://shieldthefuture.com/contact-details/*

Funders: support regular collection of accounts in the countries where public sources carry the least, and the professional build-out of FARO that makes it possible.

FARO does not sell or use anything shared with it for commercial purposes, and it removes names and any details that could identify a person or a school before publishing any part of a record. Accounts can also be shared without giving a name.

Annex 1: Reach, Additional Considerations and Methodology

This annex sets out where the records come from, what to keep in mind when reading them, and how the report was built.

Reach

This issue draws on 266 incidents from 47 countries, and 8 of the incidents do not name a specific location. Of the 266, 241 are part of the patterns featured in this issue: 193 in the four harm patterns, 215 in the five responses to harms, and 45 in the five other findings. An incident can appear under more than one pattern, so these figures overlap and should not be added together. A country counts as independent here if at least one of its incidents comes from a source other than the Human Rights Watch report.

The harm patterns are based on an analysis of these records:

- School products that open onto the whole internet: 52 incidents, 18 countries, all 18 independent
- Required school technology with no consent and no way to opt out: 110 incidents, 36 countries, 14 of them independent
- Chats and images used to expose or hurt students and teachers: 35 incidents, 12 countries, all 12 independent
- Schoolwork locked behind a paid product: 13 incidents, 7 countries, 6 of them independent

The responses to harms are based on analysis of these records:

- Inappropriate content gets in: 52 incidents, 18 countries, all 18 independent
- Required tech, no opt-out, including data taken without consent: 112 incidents, 36 countries, 15 of them independent
- Private details exposed: 29 incidents, 8 countries, all 8 independent
- Weaponization of chats and images: 35 incidents, 12 countries, all 12 independent
- Paid access to schoolwork: 13 incidents, 7 countries, 6 of them independent

The 266 incidents come from the following sources:

63 research records, 51 of them from the Human Rights Watch report

98 news articles

35 regulatory actions

25 blog or personal posts

13 court cases

17 incident database entries

14 accounts told directly to SHIELD or its partners

1 other source type

The split of incidents by country is as follows:

United States: 48

Italy: 45

India: 25

Zimbabwe: 13

Denmark: 12

Kenya: 11

9 each: Nigeria, United Kingdom

Norway: 8

6 each: Ireland, Spain

Turkey: 5

4 each: Canada, Indonesia, Zambia

3 each: Australia, Iran, Kazakhstan, Pakistan, Romania, Russian Federation

2 each: Brazil, Ghana, Nepal, Republic of Korea, Sweden

1 each: Albania, Andorra, Belgium, Bolivia, Chile, Colombia, Egypt, Germany, Japan, Malawi, Malaysia, Mexico, Netherlands, New Zealand, Peru, Portugal, Singapore, South Africa, Switzerland, Thailand, Venezuela

Not stated: 8

Additional considerations

Where published records come from. In the two patterns on student data and private details, most Danish, Italian and Norwegian records are decisions published by data protection regulators, while the US records are largely court cases and news reports. High counts from a country show where harms get written down and published, not where they happen most.

Responses to data harms. When learning products took children's data, European responses came mostly from regulators, while US responses came mostly from families and courts, along with one Federal Trade Commission order. This may reflect where regulators publish their decisions and where families can take a company to court, and not a difference in how schools or companies treat children's data.

What the responses show. The responses in this report are the ones that left a record, such as published decisions, court filings, news coverage and accounts people chose to share. The report shows what is most visible. It does not show what schools and authorities do well, or how often any response happens. Where no response is recorded, one may still have taken place.

Claims not yet decided. Three records in the first harm pattern, on school products that open onto the whole internet, describe lawsuits, those of the California girl and the Utah and Florida families, and no ruling is recorded in any of them. Eight US student-data records describe lawsuits: one ended in a settlement, two went forward to trial, and the rest had no ruling recorded.

Methodology

FARO builds each report in steps, and a person reviews and approves each step's output. AI models, mainly Google Gemini, help find sources, extract incidents, draft privacy redactions, flag possible duplicates, and propose harm labels. Incidents come from public forums, news reports, official records, published research, and direct accounts given to SHIELD and its partners. Each incident is extracted into a record, reviewed and redacted for privacy, checked for duplicates, and classified by the harm involved. The findings in this report do not consider the harm labels, only the incident summaries.

Patterns were found in two separate passes. A person read the approved incidents and identified patterns. Claude Opus, used through Claude Projects, was then given the full export of approved incidents together with written instructions and asked to propose harm patterns of its own. It was given no existing patterns, so it worked only from the incidents.

The instructions define a pattern as the way technology in ordinary use produces harm that recurs across countries, and tell the model to group incidents by that way. They were revised after earlier runs produced patterns built around something other than the way the technology affected people, such as the type of product or tool, or the role of the person harmed or of the person whose decision led to the harm.

The final instructions require each pattern to be defined by the mechanism that affected people, so that incidents involving different products or different people can belong to the same pattern. A pattern needs at least five incidents from at least three independent countries. A country counts as independent only if at least one of its incidents comes from a different source organization than the incidents from the other countries. The model could use only the incident file, with no web search or outside knowledge. It had to read every row, report how many it read, and count incidents and countries. Its proposals were marked as drafts. The person compared the model's patterns with their own and decided which were used. Patterns for institutional responses and for other findings were found the same way, each in its own Claude project with its own instructions, so the model stayed focused on one kind of pattern. Every finding in this report has been approved in the FARO database. The instructions are available on request.

The structure, wording, and conclusions of this report are the author's. Claude Sonnet was used as writing support, working section by section to check statements against the records, suggest edits, search for and propose additional sources not included in the existing incidents that might strengthen the section, and provide feedback. Claude Design was used to support the formatting of the final report.

To spot patterns across different school systems and legal frameworks, FARO uses qualitative data triangulation. FARO reads different types of information side by side: court rulings, regulatory fines, news stories, and personal accounts. Regulatory decisions and court cases show how official bodies react to harms. News stories and personal accounts capture what happens day to day, especially in places where regulators do not publish decisions or where families cannot go to court. Reading them together means that a lack of official reporting in a country does not hide the harms happening to children there.

Where records are dated, they run from 2010 to 2026. We reviewed records for this report up to 19 October 2026, and we will regularly update this report as we review new records. Changes to the recorded incidents or allocated harms patterns after that date are not reflected in this report.

FARO is a pattern-detection system, not a prevalence-measurement system. Findings should be read as evidence that a mechanism exists, not as evidence of how often it occurs in the wider population.

Annex 2: Useful Links

This annex links to FARO's submission page and incident index, the work this report builds on, help and support, measures already in place, and further reading.

All FARO Reports and Online incident index

- *https://shieldthefuture.com/faro/*
- FARO incident directory, filtered to Technology in Education: all incidents behind this report. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education
- Pattern 1: Inappropriate content gets in: incidents where school products opened onto the wider internet. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_harms=harms-pattern%3Ainappropriate-content-gets-in
- Pattern 2: Required tech, no opt-out: incidents of required products with no consent and no way to opt out. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_harms=harms-pattern%3Arequired-tech-no-opt-out
- Pattern 3: Weaponization of chats and images: incidents of chats and images used to expose or hurt students and teachers. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_harms=harms-pattern%3Aweaponization-of-chats-and-images
- Pattern 4: Paid access to schoolwork: incidents of schoolwork locked behind a product families or staff had to pay for. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_harms=harms-pattern%3Apaid-access-to-schoolwork
- Other finding: Public apps in class: classes run through everyday public apps. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_harms=other-pattern%3Aother-public-apps-in-class
- Other finding: Flagged by software: monitoring software flags that brought adults in. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_harms=other-pattern%3Aother-flagged-by-software
- Other finding: Students change grades: registers opened with a teacher's password. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_harms=other-pattern%3Aother-students-change-grades
- Other finding: Course loans: course loans that outlive the course. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_harms=other-pattern%3Aother-course-loans Other finding: Required screen time:

- daily device use with no paper alternative. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_harms=other-pattern%3Aother-required-screen-time
- Responses to Inappropriate content gets in: the incidents mentioned in these responses. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_response-pattern=response-inappropriate-content-gets-in
- Responses to Required tech, no opt-out: the incidents mentioned in these responses. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_response-pattern=response-required-tech-no-opt-out
- Responses to Private details exposed: the incidents mentioned in these responses. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_response-pattern=response-private-details-exposed
- Responses to Weaponization of chats and images: the incidents mentioned in these responses. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_response-pattern=response-weaponization-of-chats-and-images
- Responses to Paid access to schoolwork: the incidents mentioned in these responses. https://shieldthefuture.com/faro-incident-directory/?f_evidence_topic=technology-in-education&f_response-pattern=response-paid-access-to-schoolwork

Share an account with FARO

- Any harm area: https://eu.kobotoolbox.org/#/forms/a5K9fjs7jEmpz4SRRnAQ5w

Existing work named in Framing

- Human Rights Watch, "How Dare They Peep into My Private Life?" (2022). The full report, with downloads in several languages. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments
- Internet Safety Labs, 2022 US K12 EdTech Benchmark. The three findings reports, a data dashboard and ISL's school EdTech safety recommendations. https://internetsafetylabs.org/resources/reports/2022-us-k12-edtech-benchmark
- United Nations Children's Fund, EdTech for Good Framework – Version 2.0, UNICEF, Helsinki, 2026. https://www.unicef.org/digitaleducation/edtech-for-good
- Lequimboh, E., Kwaramba, R. R., Nfor, C., & Kuol, A. (2026). How prepared are African education systems for classroom content risks? Perspectives from Cameroon, Kenya and Zimbabwe (Policy Brief No. 2). Real Life Research Institute – Africa Program. https://africa-programs.reallifeinstitute.org/policy-briefs/

Help and support

- Contact SHIELD – APS for any questions, collaboration suggestions, or other help or support related to this report: https://shieldthefuture.com/contact-details/

Measures already underway

These laws, rules and guidance documents address some of the harms in this report. They are listed as they stood when the record was reviewed, without an assessment of how well they work. Each still needs its link to the official source.

- Brazil, Law 15.211/2025, Digital Statute of Children and Adolescents (ECA Digital), 17 September 2025.
- Denmark, Datatilsynet order in the Chromebook case, 30 January 2024, and Datatilsynet serious criticism of 51 municipalities in the Chromebook case, January 2026.
- India, Digital Personal Data Protection Rules, 2025, November 2025.
- Indonesia, Government Regulation No. 17 of 2025 on Governance of Electronic Systems in Child Protection (PP Tunas), 27 March 2025.
- Kenya, Office of the Data Protection Commissioner, Guidance Note for the Education Sector, January 2024.
- United Kingdom (England), Department for Education, Filtering and monitoring standards for schools and colleges, updated 16 September 2026.
- United Kingdom, Education Act 1996, section 454, as stated in a Department for Education written answer, 15 July 2025.
- United States, Federal Trade Commission, amended COPPA Rule, 16 January 2025.

Further reading

These works add context to specific patterns in this report, and one challenges part of its approach.

- **Book.** Allison Butler and Nolan Higdon, *Surveillance Education: Navigating the Conspicuous Absence of Privacy in Schools* (Routledge, 2024). The authors argue that schools are offered data collection and tracking as ways to improve outcomes and safety, even though little evidence confirms they work. Relates to: Required school technology with no consent and no way to opt out.
- **Independent research.** Center for Democracy & Technology, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI* (September 2023). This work challenges part of the report's framing. It argues that filtering and blocking online content can amount to a digital book ban, which cuts against treating filtering as the answer to school products that open onto the whole internet. Relates to: School products that open onto the whole internet.
- **Legal reference.** Council of Europe, Committee of Convention 108, *Guidelines on Children's Data Protection in an Education Setting* (November 2020). The guidelines build on a report by Jen Persson, Director of defenddigitalme. Relates to: Required school technology with no consent and no way to opt out.

- **Independent research.** Education Week and Common Sense Media, national data on students viewing pornography at school (January 2023). Relates to: School products that open onto the whole internet.
- **Guidance.** Internet Safety Labs, *School EdTech Safety Recommendations*. Relates to: Required school technology with no consent and no way to opt out, and Schoolwork locked behind a paid product.