Global Privacy Enforcement Network

GPEN Sweep Report: Children's Privacy

March 2026

Authored by the Central Sweep Coordinators:

Office of the Privacy Commissioner of Canada

Information Commissioner's Office, the United Kingdom

Office of the Data Protection Authority of the Bailiwick of Guernsey

Table of contents

Background 3

Methodology 4

Age assurance (Indicator 1) 5

- Approaches to age assurance 5
- Age assurance mechanisms observed in the Sweep 5
- Circumvention of age assurance 6
- Inappropriate content and high-risk processing 6
- What has changed over the last decade? 7
- Summary observations 7

Collection of personal information and protective controls (Indicators 2 and 3) 7

- Privacy policies 7
- Collection of personal information 8
- Protective controls 9
- Summary observations 10

Account deletion (Indicator 4) 11

- Why account deletion matters for children 11
- What Sweepers observed 11
- What has changed over the last decade? 12
- Summary observations 12

Inappropriate content and high-risk data processing and design features (Indicator 5) 13

- Exposure to harmful content 13
- When harmful content meets risky features 14
- Risks in child-targeted services 14
- Overall suitability for child use 14
- Websites versus apps 16
- Free services and child safety 16
- Summary observations 16

Conclusion 17

Appendix A 18

Background

The 2025 Global Privacy Enforcement Network (GPEN) Sweep ("the Sweep") took place during the week of November 3-7, 2025.

The Sweep examined how websites and mobile applications ("apps") used by children collect children's personal information, are transparent about their privacy practices, use age assurance mechanisms, and employ privacy protective controls to limit data collection. Some of the reviewed apps and websites are specifically designed for children, while others are used by the general population but are particularly popular among children and young people.

Today's digital space is a significant part of children's lives, offering opportunities for self-expression, learning, socialising, and connecting with their community. Online services that do not consider the best interests of children can leave young people vulnerable to risks such as online tracking, profiling, targeting, and exposure to inappropriate or harmful content.

The 2025 Sweep marked the 10-year anniversary of a similar children's privacy Sweep conducted by GPEN in 2015. This enabled a comparison of how online services protected children and used their data back then, and how they do so a decade later.

The Sweep was coordinated by the Office of the Privacy Commissioner of Canada, the United Kingdom Information Commissioner's Office, and the Office of the Data Protection Authority of the Bailiwick of Guernsey ("Central Sweep Coordinators").

Twenty-seven privacy enforcement authorities from around the world (see Appendix 1) participated in the 2025 Sweep, examining 876 websites and apps.[1]

This report is authored by the Central Sweep Coordinators. It sets out the findings and analysis of those that participated in the Sweep. It is not intended to represent the views of the wider GPEN membership or authorities that did not participate in this initiative.

The GPEN Sweep is not in itself an investigation, nor is it intended to conclusively identify compliance issues or legal contraventions. The concerns identified via this exercise may help inform targeted guidance, future engagement with organizations, and potential enforcement actions.

[1] Participating privacy enforcement authorities reviewed 464 websites and 400 apps (12 platforms were not categorized by the Sweepers). Note that Sweepers may have independently examined different versions of websites and/or apps. Therefore, the total number of distinct platforms swept may be lower.

Methodology

The goal of the Sweep was for participants, or "Sweepers," to replicate the user experience by engaging with websites and apps used by children and gather insight into the current state of their data collection and online privacy practices. This enabled us to compare findings with those of the 2015 Sweep, where relevant. While these observations and comparisons are informative, the Sweep is not a scientific study.

The Central Sweep Coordinators developed a set of instructions and associated questions to guide Sweepers' engagement with each website and app, based on the approach used in 2015. This helped ensure that Sweepers assessed websites and apps according to similar standards.

The questions focused on five indicators, which largely mirrored those from the 2015 Sweep. However, it is important to note that the questions Sweepers answered in 2025 were more comprehensive than the questions used a decade ago, which limited our ability to draw certain comparisons with previous findings. The indicators, which will be further explained in the relevant sections below, were:

1. Age assurance;
2. Collection of children's data;
3. Protective controls;
4. Account deletion; and
5. Other overall concerns.

Sweepers were asked to document their interactions with the content and features of the websites and apps – including privacy settings, privacy policies, and account creation and deletion processes – using the provided Sweep form.[2] Throughout the report, some figures exclude blank responses to specific questions in the Sweep Form, which accounts for the slight discrepancy with the total number of websites and apps examined.

Within the topic of children's privacy, each participating authority selected the focus of their Sweep – for instance, they selected websites and/or apps to sweep within specific sectors that aligned with their strategic priorities. The following chart (Figure 1) is a sectoral breakdown of the websites and apps examined in the Sweep:[3]

[2] Because the Sweep was based on the observations and interactions of Sweepers with websites and apps within a relatively short period of time (around 30 minutes), Sweepers may not have experienced and documented the full extent of content, features, and data collection of each website or app.

[3] Examples of websites and apps belonging to the "Other" sector include but are not limited to AI products, communications and instant messaging, arts and culture, entertainment, leisure, online dating, and sports news.

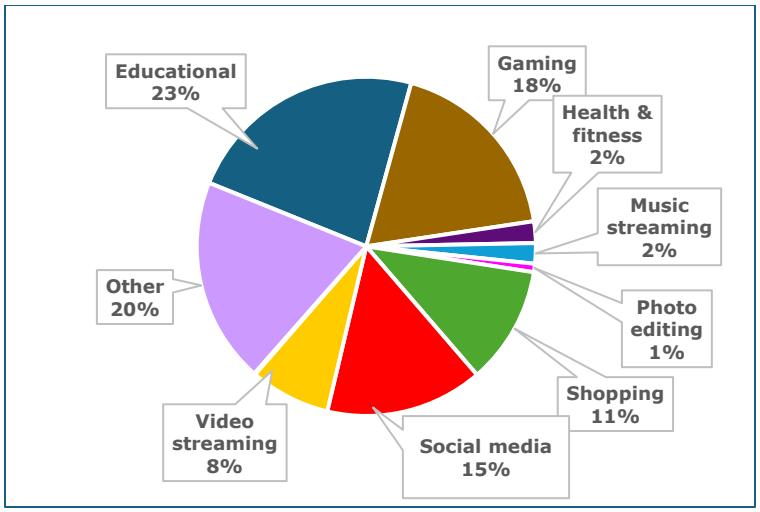

Figure 1. Sectoral breakdown of websites and mobile applications

Age assurance (Indicator 1)

Approaches to age assurance

Age assurance involves mechanisms for assessing a child's age so their access to or interactions with an online service can be tailored or restricted accordingly. There are different approaches to age assurance. Amongst others, mechanisms include:

- self-declaration (a user states their age but is not required to provide evidence);
- age verification (a user is asked to verify their age, e.g. by providing a form of ID); and
- age estimation (a user's age is estimated, often by algorithmic means, e.g. facial age estimation).

Age assurance mechanisms observed in the Sweep

Sweepers reported that the terms of service for 62% of all websites and apps reviewed (517 out of 832)[4] explicitly limited access to users over a certain age, most often 13 years of age. Of these websites and apps, 32% (164 out of 517) did not use any age assurance mechanisms at all. For the remaining 68% of websites and apps (353 out of 517) with age restrictions:

- the majority used self-declaration (88%, or 311 out of 353);
- a smaller number used age verification (11%, or 38 out of 353); and

[4] These figures exclude blank responses.

- fewer still used age estimation (5%, or 19 out of 353).[5]

Not all Sweepers reported the type of age estimation used but, where they did, this was always facial age estimation, which requires provision of a photo or video selfie.

Circumvention of age assurance

Findings from the Sweep demonstrated that self-declaration, a trust-based approach to age assurance, can easily be circumvented. [6] Sweepers reported that they were able to circumvent age assurance measures used in 72% (460 out of 641)[7] of cases; most often where self-declaration was used.

In some cases, websites and apps that used self-declaration implemented additional mechanisms to prevent access by underage users, such as simple math questions, prompts for parental consent, and preventing changes to the initial self-declared age. However, Sweepers reported that such measures were also easily bypassed, for instance by re-installing an app or clearing cookies.

Inappropriate content and high-risk processing

Given ease of circumvention, relying solely on self-declaration is unlikely to prevent children from being exposed to inappropriate content or high-risk data processing and design features where these are present in websites and apps used by children. (See pages 13 to 14 for the types of content and data processing and design features Sweepers looked for.)

Of the 34% of websites and apps (288 out of 826)[8] that Sweepers identified as having inappropriate content for children, 24% (68 out of 288) did not have age assurance mechanisms in place. However, where age assurance was implemented, 90% (161 out of 179) used self-declaration. Similarly, of the 38% of websites and apps (317 out of 824)[9] that Sweepers identified as having high-risk data processing and design features for children, 24% (76 out of 317) did not have age assurance mechanisms in place. However, where age assurance was implemented, 89% (169 out of 190) used self-declaration.

This means that children would be able to access (amongst other things) sexual images and violent content, and freely engage with other users on some websites and apps. See page

[5] These figures show the percentage of websites and apps with age restrictions that deployed each type of age assurance mechanism. Some websites and apps deployed more than one type of age assurance mechanism.
[6] Circumvention in this context refers to either easily deceiving the age assurance system or entirely bypassing it.
[7] These figures exclude blank responses.
[8] These figures exclude blank responses.
[9] These figures exclude blank responses.

Inappropriate content and high-risk data processing and design features (Indicator 5) for further findings on inappropriate content and high-risk data processing and design features identified in some websites and apps by Sweepers.

What has changed over the last decade?

Participants in the GPEN 2015 Sweep reported that only 15% of swept websites and apps used a form of age assurance. A decade later, Sweepers reported that 45% of all websites and apps (397 out of 876) deployed a form of age assurance, which represents an increase of 30%.

Summary observations

Age assurance can be a valuable part of an overall approach to protecting children and their privacy rights online. While the Sweep findings indicate an increase in the use of age assurance mechanisms over the last decade, the sole use of self-declaration (or lack of age assurance altogether) is concerning for websites and apps identified as having inappropriate content or high-risk data processing and design features for children. Where platforms are designed for or popular with children, the participating authorities encourage online services deploying age assurance to ensure that the mechanisms they use are appropriate to the risks posed to children by their platforms and that they collect the minimum amount of personal information required.

Collection of personal information and protective controls (Indicators 2 and 3)

Privacy policies

Privacy policies play an important role in enabling users to make informed and meaningful privacy decisions. A well-crafted privacy policy builds trust by setting clear expectations about how individuals' personal information will be collected, used and disclosed by an organization.

As expected, Sweepers found that most websites and apps (96%, or 825 out of 862)[10] included privacy policies. However, they identified opportunities for improvement. For example, some of the policies contained minimal information, while others were long and difficult to understand.

Sweepers also observed that 85% of the websites and apps (705 out of 825) indicated in their privacy policies that they may share personal information with third parties. This represents a substantial increase compared to 51% found in the 2015 Sweep. This may suggest that reliance on third parties may have increased, likely due to evolving revenue models, business practices and ecosystems.

[10] These figures exclude blank responses.

Collection of personal information

Sweepers found that certain categories of personal information were collected more often than others. To access the full functionality of the platforms, 50% of the websites and apps examined (437 out of 876) required the collection of usernames, 59% (519 out of 876) required an email address, and 46% (399 out of 876) required geolocation.

Other categories of personal information were collected less frequently. For example, personal interests (253 out of 876) and characteristics (257 out of 876) were collected by fewer than 30% of the websites and apps swept.

Overall, Sweepers noted an increase in the collection of certain types of personal information compared to what was observed in 2015. For example:

	2015	**2025**
Name	29% mandatory/12% optional	41% mandatory/23% optional
Phone number	12% mandatory/10% optional	18% mandatory/28% optional
Address	11% mandatory/8% optional	12% mandatory/18% optional
Photos or videos	9% mandatory/14% optional	5% mandatory/40% optional

Table 1: Comparison of personal information collection by all websites and apps swept, between 2015 and 2025

Moreover, Sweepers observed that 41% (341 out of 825) of privacy policies explicitly stated that the websites or apps did not knowingly collect children's personal information. Twenty five percent (86 out of 341) of these websites and apps were specifically targeted at children. However, Sweepers observed that some types of personal information were still collected on a mandatory basis such as the name (30%, 26 out of 86), email address (56%, 48 out of 86), username (56%, 48 out of 86) and photos or videos (5%, or 4 out of 86). Furthermore, while 54% of the websites and apps (184 out of 341)[11] making this statement in their privacy policy were not specifically targeted at children, Sweepers noted that they were still popular with, and commonly used by, children. This raises concerns about the resulting collection of children's personal information, with Sweepers reporting that many of these websites and apps mandated the collection of personal information, as shown in the chart below.

[11] Fifteen percent of Sweepers (51 out of 341) answered that they were unsure whether the website or app was targeted at children, or popular with children. Six percent of Sweepers (20 out of 341) left the response blank.

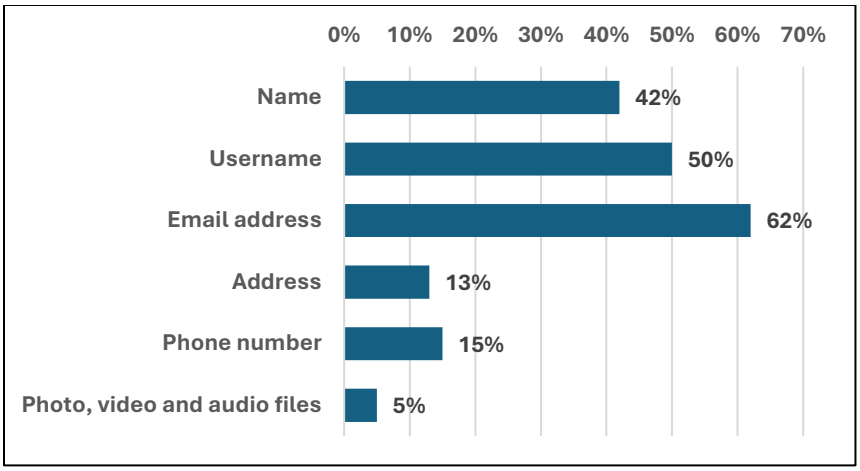

Figure 2. Mandatory collection of personal information on websites and apps, stating that they do not knowingly collect children's personal information

Protective controls

Protective controls are mechanisms implemented by organizations operating websites and apps to limit the collection of personal information to what is necessary and reduce the risk of harm to users. For example, this can be in the form of prompts for parental involvement, warnings when leaving the site, pre-made avatars/usernames, or moderated chats/message boards to prevent inadvertent sharing of personal information.

Similar to 2015, Sweepers saw good practices in the use of protective controls in 2025. For example:

- The possibility for parents to approve new people's invitations (or alternatively activate a "friend mode" where the child is free to accept new people's invitations);
- Warnings not to use real names or upload images on the website or app, such as pop-ups advising to not include personal information when choosing a username, or generation of random usernames during the sign-up process;
- The location sharing and contact access being disabled by default;
- The possibility to decline the use of location or choose to only share general location;
- The display of 'Privacy protective tips' advising users not to share personal information when interacting with a chatbot;
- Filtering posts and chats from users aged 12 and younger to prevent personal information from being posted; and
- Specifically for educational websites for children, restricting child account creation to teachers, and parental approval of content.

However, Sweepers also noted several concerning practices across many of the websites and apps. For example:

- Only 56% of the websites and apps examined (442 out of 794)[12] had the personal information collected set to private by default;
- On 47% of the websites and apps examined (393 out of the 828)[13], Sweepers were redirected to another website or app where they could be asked to disclose personal information. We note that this figure was higher in 2015 (58%);
- Seventy-one percent of the swept websites and apps (589 out of the 827)[14] did not have communications about protective controls and privacy practices tailored to children (e.g., simple language, child-friendly animations);
- Of the 38% of the websites and apps (317 out of 824)[15] for which Sweepers identified high-risk data processing and design features for children (e.g., behavioural profiling, geolocation by default, or nudging to share personal information with others), only 25% (80 out of 317) had parental dashboards and 35% (112 out of 317) had privacy communications prompting for parental involvement;
- Similarly, of the 35% of swept websites and apps (288 out of 826)[16] that featured content that could be deemed inappropriate for children (e.g., depiction of violence, hateful content, sexuality), only 35% (100 out of 288) had privacy communications prompting for parental involvement and 27% (79 out of 288) had parental dashboards; and
- As part of an overall assessment of each website and app swept, Sweepers were asked for their opinion, based on their experience using the service, on whether they would feel comfortable with a child using a website or app. The Sweepers noted that they would not be comfortable with children using 41% (343 out of 833)[17] of the websites and apps. Only 19% (64 out of 343) of these platforms were reported to have protective controls that effectively limit the collection of personal information.

Summary observations

While Sweepers identified some good examples of privacy communications and controls, they also observed concerning practices which could lead to a lack of understanding and excessive collection of children's personal information.

The participating authorities encourage organizations to ensure that their privacy policies accurately reflect and clearly explain their data handling practices, taking into consideration the potential diversity and age of their user bases. Privacy policies should be comprehensive in content and easy to understand. Platforms should also find creative and accessible ways to explain their privacy practices. Organizations can

[12] These figures exclude blank responses.
[13] These figures exclude blank responses.
[14] These figures exclude blank responses.
[15] These figures exclude blank responses.
[16] These figures exclude blank responses.
[17] These figures exclude blank responses.

empower young users and their parents by tailoring privacy communications to the intended users and making privacy controls easy to find and to use.

Organizations should carefully consider whether their collection of personal information from children is necessary and proportionate for the delivery of their services, and ensure that the privacy of young users is protected by design and by default.

Where appropriate, platforms should also encourage and facilitate parental involvement to ensure that parents can guide or support their children in making meaningful decisions about their privacy.

Account deletion (Indicator 4)

Why account deletion matters for children

Being able to delete an account easily helps children control their personal information and leave services they no longer want to use. If deletion is difficult to find or complete, children may remain on a service longer than intended, increasing exposure to unwanted content. In addition, their personal information may be retained for a prolonged period, which increases the risks of unwanted data processing in the future.

Sweepers were asked to assess whether account deletion was easy to find and easy to complete, using their judgment based on the number of steps required and the clarity of information provided.

What Sweepers observed

Consistent with the results from the 2024 GPEN Report on Deceptive Design Patterns[18], Sweepers reported that 64% of websites and apps (481 out of 755)[19] had an accessible process for account deletion (easy to find and understand), while 36% (274 out of 755) did not. In services where deletion was assessed as inaccessible (not easy to find and understand), Sweepers commonly reported that deletion options were hidden within multiple menus, users were redirected to long help pages or external support processes, or deletion required contacting customer support rather than being completed directly by the user. Sweepers described such processes as "laborious" and "practically impossible for children" in some cases.

[18] See GPEN Sweep Report 2024: Deceptive Design Patterns, July 9, 2024
[19] These figures exclude blank responses.

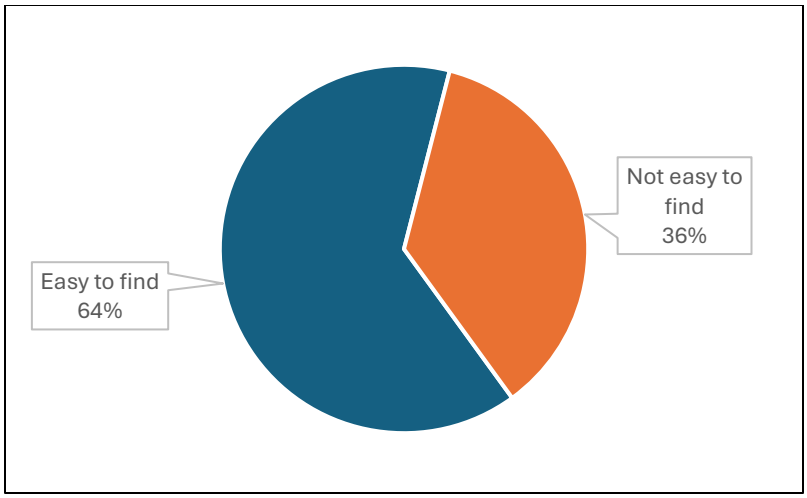

Figure 3. Ease of access to account deletion options

What has changed over the last decade?

Participants in GPEN's 2015 Sweep reported that only 29% of swept websites and apps provided an accessible means for account deletion. Ten years later, 35% more websites and apps now offer accessible deletion.

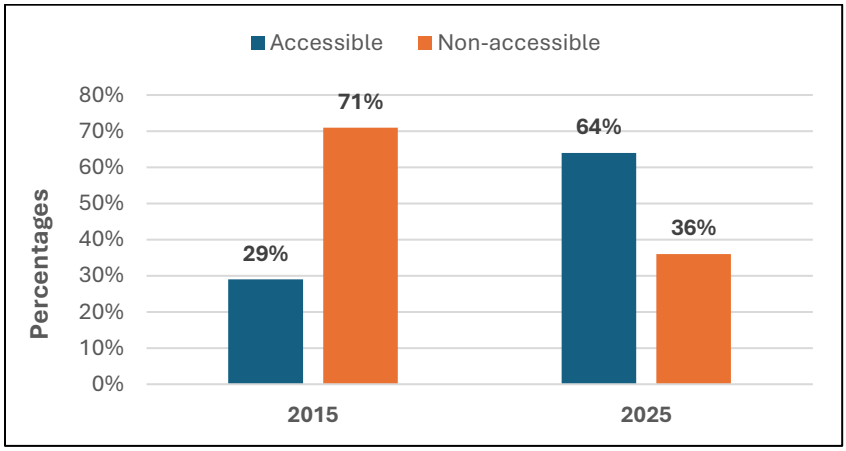

FIGURE 4. Ten-year progress regarding accessible account deletion options

Summary observations

The ease with which accounts can be deleted is an important measure of how well an individual can maintain control over their personal information. The Sweep findings show significant progress over the last decade in making account deletion options easier to find. However, over one-third of swept websites and apps still do not provide an accessible way to delete accounts. Making account deletion simple and user-

controlled remains an important part of child safety, particularly as children's relationships with online services change over time.

Inappropriate content and high-risk data processing and design features (Indicator 5)

Sweepers assessed whether websites and apps featured content that might be inappropriate for children[20], and data processing and design features that could represent a high risk to them.[21]

Exposure to harmful content

Sweepers identified concerning content across a significant proportion of websites and apps (see chart below).[22] Bullying, abusive, or hateful content was found in 15% of services (127 out of 876), while sexual content appeared in 11% of services (94 out of 876). Content related to self-harm was present in 7% of services (65 out of 876), and content related to eating disorders in a similar proportion (7%, or 64 out of 876).

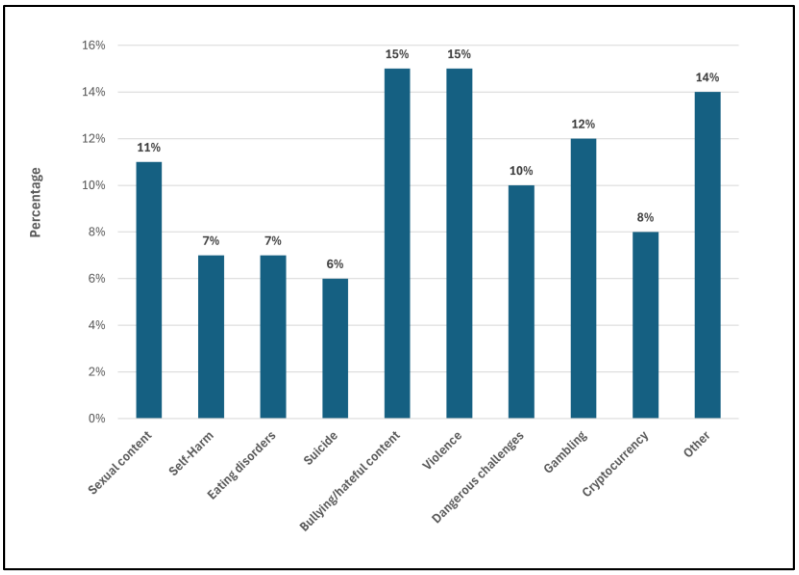

Figure 5. Proportion of websites and apps with inappropriate content, by type

[20] Sweepers were asked to record if they encountered the following types of content: sexual content; self-harm; eating disorders; suicide; bullying; abusive or hateful content; depiction or encouragement of violence; encouragement of dangerous challenges; gambling; cryptocurrencies.

[21] Sweepers were asked to record if they encountered the following data processing and design features: complex language for children; public by default privacy settings; nudging/nagging to share personal information with others; discouraging use of privacy protective options; processing of biometric data; use of behavioural profiling; geolocation on by default; ability to freely engage with other users.

[22] The chart shows the percentage of websites and apps containing inappropriate content. Some websites and apps contained more than one type of inappropriate content.

These findings demonstrate that children using some popular websites and apps risk exposure to harmful content. Sweepers noted that such content appeared in user-generated sections, chat functions, and algorithmic feeds.

When harmful content meets risky features

The combination of inappropriate content with high-risk design features may further amplify risk. For instance, when using the websites and apps and reviewing their privacy communications, Sweepers reported that behavioural profiling (i.e., tracking and analysis of user behaviour to predict interests and serve content) was present alongside self-harm content in 60% of cases (39 out of 65), and eating disorder content in 58% of cases (37 out of 64). This combination is particularly troubling, as it suggests that some platforms may not have implemented suitable measures to prevent profiling of children and delivery of content that is detrimental to their health and well-being.

Risks in child-targeted services

Sweepers noted that, in some cases, even services that are targeted at children incorporated high-risk data processing and design features. For example, Sweepers reported that 6% (18 out of 284) of such platforms employed behavioural profiling. Of these, 39% (7 out of 18) also hosted bullying or abusive content, while 28% (5 out of 18) featured depictions of violence.

Sweepers expressed concern about these findings. For instance, one Sweeper observed that a service "clearly designed for young children" included "extensive tracking of in-app behaviour with no parental visibility or control," while another noted "user-generated content with violent themes appearing in feeds alongside educational material."

Overall suitability for child use

As mentioned above, Sweepers were asked whether they would feel comfortable with a child using a website or app, taking into account both its privacy practices and any inappropriate content and high-risk data processing and design features. While it was a subjective assessment, Sweepers reported that they were not comfortable with children using 41% (343 out of 833)[23] of swept websites and apps.

[23] These figures exclude blank responses.

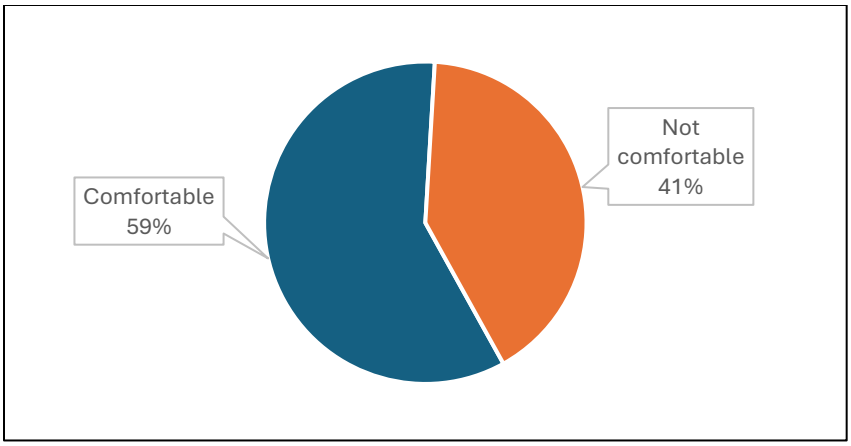

Figure 6. Overall suitability for child use

Sweepers identified a range of factors contributing to discomfort with child use. These included exposure to violent or sexual content, with Sweepers noting in some cases that services contained "content rated for ages 18 and up, with extreme violence, sex, and other themes." Sweepers also identified unrestricted interaction with other users, particularly through chat functions and community features where children could freely engage with strangers.

Design features encouraging prolonged or repeated engagement were noted, alongside monetisation practices that may place pressure on children, including advertising banners that "may direct the child to inappropriate places." Sweepers further identified profiling, tracking, and other high-risk data processing, with some reporting that tracking technologies appeared to collect information "without measures to halt collection" for child users. In many cases, more than one of these factors was present (see chart below).[24]

[24] The chart shows the percentage of websites and apps with unsuitable design features. Some websites and apps did not contain unsuitable design features.

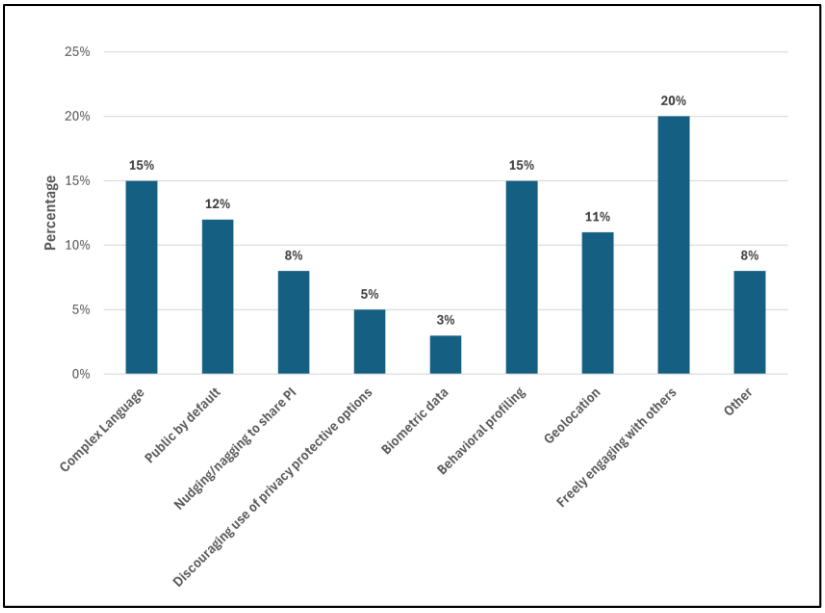

Figure 7. Proportion of websites and apps with unsuitable design features, by type

Websites versus apps

The Sweep findings show slight differences between platform types. Sweepers were generally more comfortable with children using websites rather than apps: 59% of websites (275 out of 464) were considered suitable, compared to 53% of apps (212 out of 400).

This gap suggests that mobile applications may present particular challenges for child safety, potentially due to differences in functionality, data collection practices, or interaction features.

Free services and child safety

Analysis of the data also reveals differences based on how services generate revenue. Paid services were assessed as suitable for child use in 61% of cases (117 out of 193), compared to 53% for free services (345 out of 648).

This pattern may reflect differences in business models and the incentives they create. Services that generate revenue through subscriptions may be less reliant on data-driven monetisation or engagement-maximising features that can raise concerns for children. Free services, by contrast, may be more likely to employ such practices.

Summary observations

The Sweep findings reveal that a significant proportion of services expose children to harmful content, and subject them to high-risk data processing and design features. Sweepers often reported the presence of both harmful content and high-risk design

features within the same service, potentially amplifying risks to children. Where websites and apps are used by children, the participating authorities encourage online services to design these platforms in a way that is appropriate for their use, including ensuring that the content children encounter and the features made available are age appropriate.

Conclusion

The purpose behind the GPEN Sweep is to encourage organizations to comply with privacy and data protection legislation, while promoting co-operation between privacy enforcement authorities across the globe. Though the Sweep is not in itself an investigation, nor is it intended to conclusively identify compliance issues or legal contraventions, the concerns identified via this initiative may help support targeted advice, engagement with organizations and/or enforcement actions in the future.

The outcome of this year's Sweep shows mixed results. Across many websites and apps, Sweepers observed good practices to protect children and their personal information. However, Sweepers also noted practices that raise concerns about children's privacy, and that suggest some risks may have increased over the last ten years.

For instance, compared to 2015, more online services designed for or used by children now require users to provide their personal information to access the full functionality of the platform or share their personal information with third parties. Additionally, while the use of age assurance mechanisms to restrict children's access or interaction with online services has increased, Sweepers found that such measures were often easily circumvented. This is concerning in instances where websites and apps had inappropriate content and/or high-risk data processing and design features for children.

All individuals should have their personal information protected, particularly children who navigate the digital space and use online services. By adopting child-friendly practices, such as limiting the collection of personal information, designing the services to be privacy-protective by design and by default, and using age assurance mechanisms appropriate to the level of risk on their platforms, organizations can contribute to children's well-being online.

Appendix A

The following privacy enforcement authorities provided their results:

1. Office of the Australian Information Commissioner
2. Office of the Privacy Commissioner for Bermuda
3. Agência Nacional de Proteção de Dados, Brazil
4. Office of the Information and Privacy Commissioner of Alberta, Canada
5. Office of the Information and Privacy Commissioner for British Columbia, Canada
6. Office of the Privacy Commissioner of Canada
7. Information and Privacy Commissioner of Ontario, Canada
8. Commission d'accès à l'information du Québec, Canada
9. Office of the Privacy Commissioner for Personal Data, Hong Kong, China
10. Personal Data Protection Bureau, Macao, China
11. Estonian Data Protection Inspectorate
12. Commission Nationale de l'Informatique et des Libertés, France
13. Gibraltar Regulatory Authority
14. Office of the Data Protection Authority of the Bailiwick of Guernsey
15. Isle of Man Information Commissioner
16. The Privacy Protection Authority, Israel
17. Garante per la Protezione dei dati personali, Italy
18. Personal Information Protection Commission, Japan
19. Jersey Office of the Information Commissioner
20. Office of the Information and Data Protection Commissioner, Malta
21. Autoriteit Persoonsgegevens, Netherlands
22. Office of the Privacy Commissioner of New Zealand
23. Datatilsynet, Norway
24. National Privacy Commission, Philippines
25. Information Commissioner of the Republic of Slovenia
26. Information Commissioner's Office, the United Kingdom
27. California Privacy Protection Agency, the United States of America