香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong
PCPD.org.hk

保障、尊重個人資料
Protect, Respect Personal Data

Collection and Use of Personal Data through the Internet – Points to Note for Data Users Targeting at Children

The Privacy Commissioner for Personal Data has published the **"Guidance for Data Users on the Collection and Use of Personal Data"** [1] through the Internet for data users when they engage in online activities that involve personal data.

This leaflet seeks to highlight certain essential aspects relevant to data users who interact with children (for the purpose of this leaflet, children are generally referred as those aged under 18) via the Internet, and are likely to collect their personal data via online means. It is therefore relevant to those who operate online platforms (including websites, forums, mobile apps, etc.) where, for example, the underlying goods or services are targeted at or popular among children.

The Special Needs of Children

Children are often identified as a vulnerable group who have special requirements in privacy protection, particularly in the context of online activities.

Children are more inclined to follow instructions without questioning, less privacy-aware and less able to exercise caution when communicating online. Even if warnings are given, children are often unable to appreciate the full ramifications of over-disclosure or over-sharing of their personal data, and those warnings are invariably disregarded.

Furthermore, organisations that **"protect, respect personal data"** of children will win their teachers' and their parents' trust, as well as demonstrate a commitment to satisfy their social responsibilities and will likely gain a competitive advantage over their peers.

The advice

When interacting with children, data users should bear in mind children's vulnerability and consider adopting the following age-appropriate approaches to make sure that they protect and respect children's personal data.

[1] See www.pcpd.org.hk//english/resources_centre/publications/files/guidance_internet_e.pdf

Collection of personal data

Avoiding (instead of just limiting) the collection of personal data

Instead of just limiting the types and amount of personal data to be collected, data users should also consider the best practice of not collecting any personal data from children altogether, given that children may not fully understand all the privacy risks and may not know whether they should or how to refuse providing personal data. This is particularly relevant in relation to personal data that is more sensitive in nature, such as that related to health, biometrics, etc.

Collection of third party's (such as their parents' or friends') personal data from children (particularly younger ones at primary school age and below) may be regarded as unfair in some circumstances.

Best Practice Tips

- Instead of showing a complex online form comprising both mandatory and optional fields, a two-part form should be used to clearly group mandatory and optional fields separately. This will also prompt data users to reconsider if they should avoid collecting the optional data;
- Avoid open-type questions in online forms by which children may feel more inclined to over-supply information to data users;
- "Just in time" reminders or warning messages may be adopted in the online form to alert children of the minimum amount of information they are expected to supply; and
- When collecting information about third parties (such as parents or friends), children should be explicitly reminded that they need to consult and obtain consent from those people before providing their personal data.

Offering of discussion forum

Although data users who offer discussion forums to children may believe forum contents are posted by children voluntarily, they should still ensure that children understand the privacy implications.

Tips

- When offering discussion forums to children, data users should ensure that children know, prior to taking part in any discussion, who else may join the forums and have access to all the discussions, whether the forums are monitored/moderated by the data users, and whether discussions can take place among a specific group of users, etc.; and
- Deletion and editing of posts should be offered so that children have a second and considered chance to change their minds or alter the content after posting.

Best Practice Tips

- Data users should offer discussion forums that would enforce previewing of contents before they are posted, in order to encourage children to think twice before posting; and
- Data users should remind children that, despite the ability to delete posts and to use restrictive privacy settings on the forums to limit sharing, any other members they permit to access that information may easily copy and repost the information to public forums in a way that the children would have no control over.

Getting parental involvement

Data users should encourage children to involve their parents or teachers when collecting personal data from them. This will not only earn the trust of the children, but also of their parents and teachers. As a result, this will help strengthen the reputation of the data users.

Best Practice Tip

- Data users should ask children, particularly younger ones at primary school age and below, to consult parents or teachers when providing their personal data online.

Deleting account or personal data

Children may be ready to experiment with new online platforms but may not be aware of their rights to have personal data removed. If such a removal process is cumbersome, children may not be able to understand it. Data users should, therefore, ensure that children are well informed of their rights and offer them with an easy and online way to completely remove personal data they have supplied to the data users or disclosed on such platforms.

Tips

- If an online platform requires children to create accounts before using its services, data users should offer a readily accessible and user-friendly means for account holders to remove the account and all associated data collected by the data users;
- Similarly, even if the child does not need to create an account, but the data users nevertheless collects his personal data by online means, data users should inform him of the collection of data and his relevant rights, as well as providing an online means for the child to request the deletion of collected personal data; and
- As a best practice, data users offering forums to be used by children should provide means for children to delete the contents they have posted before removing their accounts.

Use of personal data

Default setting

Children may not be aware that they could check or change all the privacy settings before using online platforms. Data users should therefore ensure that default configurations are pre-set with privacy protection in mind, and inform children accordingly.

Best Practice Tip

- In the case of online platforms that involve the sharing of information between users or members of the public, the default setting for all sharing should be as restrictive as possible. There should be sufficient notice and explanation to the children on the implications of setting and making changes to these settings.

Disclosure of personal data

On online platforms where children's personal data is to be published, data users should be mindful of providing clear notice to children on or before collecting the data, as well as limiting the audience of such information to those who have a genuine need to access that information. Data users should also consider using pseudonyms to identify individuals. As a best practice, data users should provide means to enable children to opt-out of such publication.

Tips

- When posting participant lists for sporting events, data users should use pseudonyms (such as participant number), limit any other information to be disclosed (such as identity card number, date of birth, etc.) and/or limit the accessible audience to the smallest group possible; and

- When posting event photos, data users should do this in a respectful manner and ensure that all participants are informed of the arrangement before pictures are taken and, as a best practice, offer an opt-out mechanism.

Change of use

If data users wish to change the use (including disclosure) of children's personal data, they must obtain prior consent from the children.[2]

Tips

- If schools or educational institutions have not made it clear to children that they would post their examination results online, they should obtain consent before doing so. Alternatively, schools or educational institutions may consider publishing the overall examination results without identifying a particular individual.

[2] Parents may give consent on behalf of children as appropriate or necessary, and where the parents have reasonable grounds to believe that the use of the personal data for the new purpose is clearly in the interest of the children.

Interaction with social networks

When data users require or allow children to use their social network accounts for interaction (such as logging in, using "like", "share" or similar action that may show the children's social network account names) with their online platforms, the children may not be aware that this interaction can be seen by other users of the social network or the online platform. In many cases, the data users or others may be able to collate/combine information from the social network and the online platforms to profile or identify the children. Data users should explain clearly to children the implications of using social network accounts.

Best Practice Tip

- Data users should offer either anonymous log-in or allow children to create separate accounts (instead of requiring or allowing the use of social network accounts) on their online platforms.

Redirection to other sites

As a best practice, when an online platform redirects children to another site, clear notice should be given to the children. This is particularly important when the redirected site is not under the direct control of the same data user. In the absence of such notice, children run the risk of unintentionally or unknowingly disclosing their own personal data.

Best Practice Tip

- When redirecting children from one online platform to another, data users should display a message telling the children details of the site they are being redirected to, and its relationship with the data users (such as a subsidiary or related company, an organiser of events, etc.).

Direct marketing activities

The Ordinance prescribes circumstances where direct marketing using personal data are permissible. Data users should be mindful that, even for non-profit making purposes, the promotion or advertising of services (including solicitation of donation) is considered as direct marketing activities. They should familiarise themselves with the requirements before conducting any direct marketing activities. Data users should, therefore, refer to the 'New Guidance on Direct Marketing' [3] issued by the Privacy Commissioner for Personal Data for details.

For example, data users who intend to use a child's personal data in direct marketing, must inform the child accordingly, obtain his prior consent[4] and provide him with a channel through which his consent may be communicated.

Data users should note that even adults sometimes have problems navigating the various clauses and consent forms of direct marketing, therefore expecting children to understand their rights in direct marketing may be unrealistic.

[3] See www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf

[4] In the context of direct marketing, the meaning of the word "consent" includes an indication of no objection.

Best Practice Tips

- Data users should seek consent from children on whether they wish to receive direct marketing messages (for example: students at an extracurricular painting centre should not be sent direct marketing messages related to dancing, drama or language studies classes, etc. unless their prior consent is obtained);
- Instead of using direct marketing as a means to promote their goods and services, data users should consider displaying advertisements on their online platforms that are not based on the profiling of children; and
- If it is necessary for data users to engage in online direct marketing activities with children, they should offer children an easily accessible online means to opt out of the direct marketing messages.

Security of personal data

Personal data protection is no child's play

Even though some online platforms targeting at children may be of a social or leisure nature, data users still need to be serious about the protection of personal data collected. Any wrongful disclosure or misuse of personal data may have dire and long-term consequences as children may not be able to protect themselves from fraudulent activities.

Tip

- Data users should not consider its online platform to be of trivial nature and thus be lax about data security. Data users must conduct risk assessment to determine the risk of security breach and the harm that it may cause.

Transparency in privacy policy and practice

Age-appropriate language and presentation

The ability of children to understand the privacy implications of the often legalistic and lengthy privacy policies depends also on their age and cognitive development. Hence, data users should always keep the target audience in mind in their choice of language and presentation.

Best Practice Tips

- A privacy policy that is legalistic is unlikely to be understood by children;
- If data users offer services over an online platform that targets different age groups, a single version of the privacy policy is not likely to ensure that it will be easily understood by children of various age groups. Data users should develop different age-appropriate versions of the privacy policy targeting at different age groups; and
- Data users may deploy user-friendly means to present the written privacy policy, for example by utilising graphics and animation. Consents or opt-in obtained through age-appropriate communication means would be encouraged.

Privacy controls (or dashboards)

Data users should consider providing a single place on their online platform for children to find out what personal data has been collected or maintained.

Best Practice Tips

- Data users may provide a "dashboard" for children to see, change and remove all the postings (where applicable) and the personal data collected. The same dashboard may also include all the privacy related settings (such as whether the children allow certain personal data to be used, shared or seen by others) for ease of use; and

- Especially for younger children, data users may extend such dashboards to parents so that they can help younger children to manage their own personal data privacy.

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**