An Chomhairle Mhúinteoireachta
The Teaching Council

Response to DATA PROTECTION COMMISSION Public Consultation

on the processing of Children's personal data and the rights of children as data subjects under the General data Protection Regulation

The following submission is made on behalf of the Teaching Council to the Data Protection Commission (DPC) in response to the public consultation on the processing of children's personal data and the rights of children as data subjects.

The Teaching Council is the professional standards body for the teaching profession, which promotes and regulates professional standards in teaching. It acts in the interests of the public good while upholding and enhancing standards in the teaching profession. The focus of the Council's work is towards teachers and with the exception of the Council's Fitness to Teach function which deals with complaints made against teachers, the Council does not deal or interact with children or data relating to children. The Council has a specific statutory responsibility to have regard to the need to protect children and vulnerable persons.

The Council's submission to the DPC will therefore focus on the Fitness to Teach function where there can be interaction with children as complainants and witnesses, or children may be referenced in materials associated with a complaint made against a teacher. As a result of this the Teaching Council may hold personal data relating to children.

The submission includes responses to those questions posed in the public consultation document considered relevant to the work of the Teaching Council.

Q1 – *What methods could organisations who collect and use children's personal data employ to easily convey this transparency information to children?*

To date the Teaching Council has not put in place specific communications mechanisms for conveying information to children and young persons. The Council has sought to make all publicly available communications material concerning fitness to teach complaints as simple and as readable as possible. One proposal that has been made is to use images or animated images in communications material. The Council has used this approach very successfully to explain processes such as applying for Garda vetting and electronic voting in Teaching Council elected member elections. While the audience in these instances were adults, it has potential to be used for children.

Q2 – *What approach should be used by organisations whose products or services are aimed at both adults and children? For example, should two separate sets of transparency information be provided that are each tailored according to the relevant audience?*

As noted in Q1, children may wish to access information on how to make a complaint against a teacher. A separate more visual approach to conveying key information and concepts is worth considering in addition to the existing website material. This approach would better match the differing information needs to children's ages and capacity.

Q3 - *At what age or in what circumstances should a child be able to make an access request to an organisation and receive a copy of their personal data? Is age the only relevant factor and if not, what other factors should be taken into consideration?*

It is difficult to identify a particular age although there is a natural boundary around age 12/13 when children progress from primary school to post-primary school. Perhaps, no age should be specified but that a set of criteria for assessing the release of data in response to an access request might be developed. Criteria might include capacity of the child to understand the data being released, the potential for an adverse impact on the child if the data is released, the nature of the data being held on record, whether medical or health matters are involved, the potential for partial release of data, etc.

Q4 - *In what circumstances should a parent be able to make an access request and receive a copy of their child's personal data? Is there an upper age limit after which a parent should not be able to make an access request for their child's personal data? Are there circumstances where both the parent and the child should have to jointly make an access request for the child's personal data?*

It is suggested that a parent should be allowed make an access request and receive a copy of their child's personal data until the child is 18 years of age. It is also suggested that from age 16, a request for personal data of a medical nature should be made jointly because by law, patients aged 16 years and over are entitled to give consent to surgical, medical or dental treatment (*except psychiatric treatment which remains aged 18 years for consent*);

Q5 – *How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy when organisations are dealing with access requests for the child's personal data?*

Please see response to Q4 above. Where possible, the views of the child should be sought and considered particularly where the child has reached the age of 12/13 as noted in the response to Q3.

Q6 – *At what age or in what circumstances should a child be able to make an erasure request to an organisation and have their personal data erased? Is age the only relevant factor and if not, what other factors should be taken into consideration*?

Organisations should have a data retention policy which makes clear if, when and under what circumstances personal data should be retained and erased. The age of the child should not be the only determinant. The policy should take into account:

- The organisations role;
- The reasons for the holding of data in the first instance;
- The potential for future use of the retained data (In the case of the Teaching Council, consideration would have to be given to whether there are potential child protection or safety risks associated with not retaining the data);
- The balance between the child's right to privacy and a public interest (including protection of the child) reason for retaining the data.

Q7 – *In what circumstances should a parent be able to make an erasure request on behalf of their child and have their child's personal data erased? Is there an upper age limit after which a parent should not be able to make an erasure request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an erasure request*?

A parent making an erasure request on behalf of their child should be considered in the context of an organisation's Data Retention Policy generally and the criteria suggested in the response to Q6. Beyond the age of 18, a parent should certainly not be entitled to make an erasure request regarding their child's personal data unless the child, once they reach the age of 18, is suffering physical or mental health difficulties which render that person unable to make a request for erasure themselves. A parent could request erasure of a child's personal data on the death of a child perhaps once this in line with an organisation's data retention policy and once the child's death is not the subject matter of an ongoing investigation by the particular organisation. Again, a joint request could be considered for erasure of personal data of a medical nature where a child is between the ages of 16 and 18;

Q14 – *What measures should organisations take to incorporate the principles of data protection by design and by default into the services and products that they offer to children*?

Redacting direct contact details of children and names or third party children where appropriate. It depends on the organisation's role and functions and the services that they provide. The following additional internal processing measures might also assist:

- Having a well-defined Privacy Statement
- Safe methods of electronic transfer of data e.g. password protection, OneDrive, ShareFile
- Restrictions on access to data by internal staff;

Q15 – *Do you think products/services that are used by or offered to children should have built-in default settings that vary according to the age and evolving capacities of a child? For example, should there be a stricter privacy settings for younger children? How should these variations in the privacy settings be given effect*?

While in principle it would seem appropriate that stricter privacy rules apply to younger children, the fact is that a 6 year old and 14 year old are both children in the eyes of the law and should be treated similarly in terms of privacy. The management and monitoring of privacy arrangements based on age could be very difficult to implement. In summary, for practical reasons a similar privacy settings should be applied to all children.

Q 16 – *Are there any other particular issues you would like to raise with the DPC in connection with the subject matter of this consultation*?

No further comments.

4 February 2019