Submission from the Association of Community and Comprehensive Schools (ACCS) to the Data Protection Commission (DPC) on the "Fundamentals for a Child-Oriented Approach to Data Processing".

Who we are and what we do:

The role of the ACCS is to promote and represent the 96 Community and Comprehensive second-level schools in the Republic of Ireland. ACCS leads and supports the Boards of Management of our schools to provide equal access to a comprehensive, co-educational, community-based, multi-denominational education. In doing so we aim to contribute to a just and caring society.

As a key stakeholder in relation to processing children's data we wish to make a submission/provide our feedback and comments on the DPC's document *"Fundamentals for a Child-Oriented Approach to Data Processing"* (**Fundamentals**).

Having reviewed the Fundamentals we have identified that most of them relate to **online** services either targeting children or accessible to children. However, we note that it is the DPC's intention that their guidance will relate to both online and **offline** processing of children's data. The Fundamentals will therefore be applicable to schools.

1. **The key proposed Fundamentals that are relevant to our schools are:**

    a. Information in every instance

Children are entitled to receive information about the processing of their own data.

    b. Child-Oriented Transparency

The information provided must be in a concise, transparent, intelligible and accessible way, using clear and plain language that is comprehensible and suited to the age of the child.

    c. Let Children have their say

The DPC considers that a child may exercise their rights at any time as long as they have the capacity to do so and it is in their best interests.

    d. Consent does not change childhood

Consent obtained from children or from the parent/guardian should not be used as justification to treat children of all ages as if they were adults.

Comment from ACCS in relation to Fundamentals:

ACCS welcome the above and note that to meet the standards we may need to update our policies to be more child oriented. We may also require further training to school management and staff on the importance of providing access to data to children while balancing those rights with the welfare and best interests of the child.

2. **Recommended Measures**

The Fundamentals have also identified some practical recommended measures to create safer environments for children's data. Most of these relate to service providers, and it is our view these

are the standards that our schools should expect from app developers, or third party software providers when asking them to process children's data on their behalf.

Crucially, we also see many of these applying to ours schools when offering remote learning:

2.1 The key recommendations which relate to our schools are as follow:

a. DEFAULT PRIVACY SETTINGS – **Ensure the strictest privacy settings apply to services directed at/ intended for, or likely to be accessed by, children.**

b. DATA MINIMISATION – **Minimise the amount of data collected from children in the first instance** and throughout their interaction with a service and/or minimise the subsequent use and sharing of the data. Reduce the level of granularity of data types collected from children to avoid specificity and accuracy wherever profiling occurs, could occur or may occur in future.

c. SHARING AND VISIBILITY – **Do not systematically share a child's personal data with third partie**s service providers without clear parental knowledge, awareness and control.

d. GEOLOCATION – **Turn off geolocation by default for child users on devices supplied by schools,** unless a service being provided is necessarily dependent upon it; if this is the case, make it clear to the child (e.g. through the use of symbols/ icons) that their location is available to the service or can be seen by other users. Provide clearly visible controls to allow the child to change this at any time or following each session, after a short time period, or once the event or feature requiring location has completed. Significantly reduce the level of accuracy of geolocation data collection except where necessary.

e. DEVICE-LEVEL PROCESSING – **Opt to process personal data on the user's device, as opposed to transferring the data to the cloud.**

2.2 When assessing a 3rd party application for use in our schools, the standards to look for should include:

a. PARENTAL DASHBOARD – **Where appropriate, provide parents with an overall view of activity (including any history of activity) and settings that their child has available to them**. Child accounts should have available information on the functionality of such dashboards.

b. PARENTAL TRACKING/ MONITORING – Where service/ device settings allow for parents to track or monitor their child's use of online services (such as with a parental dashboard, where appropriate), transparency settings should apply so that it is visible to the child that their

parent(s) can tell which app/ website/ program etc. they are using or that their parent(s) can later review their activity history.

c. INTERVENTION – Where service/ device settings allow for parents to track or monitor their child's use of online services, **consider allowing parents to modify child account controls and settings,** where appropriate. Provide notifications to parents when these settings are altered, especially where location, biometrics or device sensors are involved. Ensure access to such a dashboard by parents is secured with multiple factors of authentication.

d. RISK MANAGEMENT – **Make consideration of processing of children's personal data a requirement in all DPIAs**. This should include access control restrictions for adults to child audiences or child-oriented areas of a service.

e. SECURITY – Consideration of children as an audience and the risk factors associated with processing children's personal data should be a priority when creating, updating or maintaining security controls, measures and "threat models". This may mean making controls easier to use while maintaining the same high level of security. Alternatively, it may mean making controls only available to parents. Default settings for such controls should ensure high levels of security rather than more relaxed levels that may be available to adults. Higher security settings for child account data may be appropriate, including the possibility of isolating or "air gapping" child personal data from adult personal data. Administrator accounts for child data should be flagged or have a specific role so that internal organisational access can be easily distinguished, monitored, audited and altered.

f. BREACHES – **Notification** procedures in cases of personal data breaches should account for notification **to the parent rather than the child, where appropriate depending on the age of the child user affected.** Breach records maintained by an organisation and notified to the DPC should include references to any involvement of children's personal data.

g. BIOMETRICS – **Avoid the collection and processing of children's biometric data.**

Comment from ACCS in relation to the Recommendations:

ACCS notes that in the remote learning environment, many of the online relevant recommendations may also apply to our schools. While anything which creates a safer environment for children and their data is welcomed by ACCS, the realm of remote learning is still a steep learning curve for schools, and an education piece will be required for ACCS to meet the standards expected by the guidance.