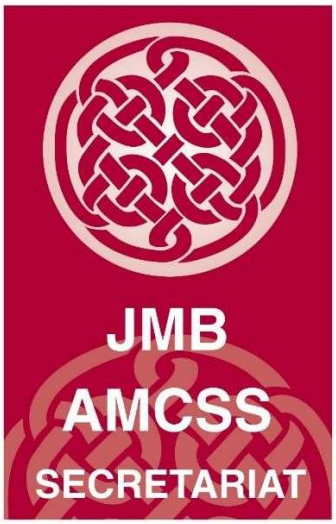

Joint Managerial Body

Submission

Public Consultation by the Data Protection Commission on
Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing

31st March 2021

Contact: [redacted]

[redacted] www.jmb.ie

SUBMISSION

Public Consultation by the Data Protection Commission on *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing ("The Fundamentals").*

The Joint Managerial Body (JMB) was founded in 1964 to represent the interests of all voluntary secondary schools in the Republic of Ireland. It is the main decision-making and negotiating body for the management authorities of almost 380 voluntary secondary schools. The JMB comprises two founding organisations: AMCSS, the Association of Management of Catholic Secondary Schools and the ISA, the Irish School Heads' Association, representing the Protestant Schools in the State.

There are approximately 180,000 students in our schools ranging from age 12 to 18 years.

Emphasis on children's data is welcomed

The JMB welcomes the publication of the Fundamentals also the attention that the Data Protection Commission (DPC) has given in recent years to the processing of children's personal data.

The JMB believes that in any matter relating to children, the child's best interests are of paramount importance and is pleased to see that this perspective is appropriately reinforced throughout the Fundamentals, as captured in this statement on page 19: *it is clear that the obligation deriving from international and EU law to act in the best interests of the child is paramount when considering the position of children as data subjects and in any context where decisions are made by any organisation in connection with the processing of children's personal data.*

Furthermore, it is welcomed that the Fundamentals emphasise the fact that data protection is not a barrier to safeguarding and that child protection/welfare considerations should always take precedence.

Greater transparency should be a priority

It has been well documented that many controllers, particularly organisations who regularly process children's data for purposes relating to social media etc., need to enhance their transparency offerings so that children have a better understanding of how their personal data is being used.

The legislation recognises that children may be more exposed to risk as a consequence of their age. The concerns around inappropriate sharing of children's images by social media and elsewhere are well documented. Organisations who are processing the personal data of children need to recognise their responsibilities in this regard.

It is often difficult for adults who are seeking to assist children with the exercise of their data protection rights, to identify the appropriate contact channels. These difficulties are certainly no less when children are trying to exercise their rights themselves, for example, their right of erasure with regard to the deletion of personal data (images, videos etc).

JMB would also strongly endorse the view set out in the Fundamentals (p30) that organisations who process the personal data of children should be both easy to contact and also more responsive in terms of the speed and efficacy with which concerns are addressed.

There is also significant potential for organisations to use alternative modes of communication (e.g. audio, video, graphical modes) to supplement, or in some cases replace, the use of written notices. The publication by Data Protection Authorities of standardised icons (as promised under GDPR Article 12) would assist organisations in this regard.

The exercise of Children's Rights

JMB welcomes the focus given in the Fundamentals to the exercise of children's rights, particularly that discussed in section 4.2 (p35-36) where the issue of a parent or guardian seeking to act on behalf of a child is addressed. It is helpful that the DPC provides a (non-exhaustive) list of factors to be considered by an organisation in deciding whether it is in the best interests of the child that their parent(s)/ legal guardian(s) step into their shoes and exercise their data protection rights. Further development of this advice, and its possible formulation into a Code of Practice, could be very helpful for schools and others who are required to manage access requests in familial situations that are sometimes complex and fraught circumstances.

Greater expectations needed of Processors

A significant quantity of school data processing is now undertaken by third party service-providers i.e. where the school as controller enters a contractual arrangement with organisations who act as data processors on behalf of the school.

Our schools understand their responsibility to ensure that any processors they appoint reach the appropriate standards (and satisfy, for example, the requirements of GDPR Article 28). However the reality is that those organisations who act as processors often have access to much greater resources (financial, human, knowledge etc). It is also the case that, schools usually have only limited opportunity to influence the functionality of the processing services that they are offered.

JMB believes that it could be beneficial if some means were found of extending the reach of GDPR Article 25 (Data Protection by Design and by Default) so that its requirements were applicable not just to controllers but also to those who are acting as processors and providing commercial products that relate to children's data. This could help to ensure that, as stated in the Fundamentals (p58), *data protection measures should be built into the architecture and functioning of a product or service from the very start of the design process (rather than being considered after the development phase) and that the strictest privacy settings should automatically apply to a product or service.*

Similarly, the burden of responsibilities that stem from GDPR Article 35 (Data Protection Impact Assessments) might be better shared between controllers and processors. For example, processors might be required to populate a template DPIA with relevant information which is then made available for completion by the controller i.e. the school. The resource imbalance that exists between schools and commercial service providers means that it is often difficult, if not impossible for schools to impose their own expectations around appropriate contractual due diligence. Again, the reality is that schools can often be under pressure to operate on a take or leave basis when it comes to entering contractual arrangements. A basic requirement should be that all data processors are required to offer a significant level of detail in clear non-technical language that makes explicit the description of the data processing, the identity of all sub-processors, any data export to countries outside the EEA and the applicable safeguards, as well as an comprehensive listing of the security guarantees and measures that are in place.

During Covid-19, there has been an expectation that our schools increase their provision of remote services to learners. In such circumstances, schools can come under pressure to adopt at short notice,

products that are perceived to enhance their capacity to deliver remote instruction. It would greatly benefit our schools if supervisory authorities were in a position to exert greater influence on the default embedding of the highest standards with the suppliers of "edTech" solutions.

This trend has accelerated further over the past year with the increased adoption for example of various tools, video-conferencing software, to support the delivery of remote online learning. To quote the Council of Europe, *Distance learning tools and resources should be subject to the same rigorous due diligence for pedagogical quality, safety and data protection standards, for instance regarding the default settings, so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default). Processing must not involve more data than is necessary to achieve the legitimate purpose* (Council of Europe Guidelines on Children's Data Protection in an Education Setting, November 2020).

As the use of technology-based solutions offering learning and administrative support to schools seems only likely to accelerate further in the years ahead, a Code of Conduct or Code of Practice governing the processing of children's data by such companies would be of benefit. Ideally such a Code would be established on a statutory basis, and demonstrated compliance would help to provide the necessary reassurances for both schools and learners.

Issues related to Consent

Some commentators on online learning are of the opinion that the *Digital Age of Consent* is always applicable where schools are offering remote services to learners. The digital age of consent only relates to bodies who are offering information society services (ISS) directly to a child and who choose to rely on consent as the lawful basis for doing so.

If a school is using an online platform to support teaching and learning, they are very often relying on the fact that the data processing is necessary for compliance with a legal obligation or a task carried out in the public interest i.e. processing activities that stem from the school's obligations to deliver public education. In general, a school will rarely rely on the consent of data subjects to process their data for these educational purposes.

In some circumstances operators of software platforms expect schools to confirm that user (usually parental) consent has been obtained. Sometimes this expectation appears to stem from requirements that apply to service providers in the US under COPPA (Children's Online Privacy Protection Act) legislation. JMB's view is that where a software solution provider is acting as data processor it isn't appropriate that they seek to determine the lawful basis as this responsibility should be reserved for the controller i.e. the school.

Conclusion

In conclusion, the significant work that underlies the production of the draft Fundamentals is evident and greatly welcomed, particularly in view of all the competing demands for the limited resources that are available to the Data Protection Commission. JMB recognises and applauds the priority that is being given to the protection of children's personal data and looks forward to contributing further to this important work as it proceeds further in the time ahead.

[redacted]

31st March 2021