GDPR
In Schools

A Response to Age Appropriate Design: a code for online services

Author: Tony Sheppard, CIPP/E: Head of Services
Version: 1.0
Revision Date: 31/05/2019
Classification: Protected
Team: M Management
Programme: ICO
Unique Doc Reference : 4
Uncontrolled if Printed or Exported

Important Notice:

The contents of this documentation are the confidential information of GDPR in Schools Limited and are subject to the provisions of GDPR in Schools Limited's standard Customer Agreement or Non-disclosure Agreement (as relevant) or any similar agreement signed by GDPR in Schools Limited and entered into with the recipient. The contents of this documentation (or any part or it) must not be used or disclosed to any third party by the recipient except as expressly permitted by the relevant agreement. If you (or your company) have not signed an agreement with GDPR in Schools Limited you must not use this documentation, must treat it as strictly confidential and must promptly return it to GDPR in Schools Limited. Any unauthorized disclosure of the Information may give rise to a right by GDPR in Schools Ltd to take legal action against the discloser and/or the Client for any losses, claims, damages or liabilities arising out of such disclosure.

Document History

Version History

Date	Version	Author	Comment
31/05/2019	1.0	Tony Sheppard	Published document

Review History

Date	Version	Author	Role
31/05/19	1.0	Tony Sheppard CIPP/E	Head of Services
31/05/19	1.0	Lynne Taylor	CEO

Table of Contents

Document History 2
Version History 2
Review History 2
Table of Contents 3
1 Outline 4
2 Key Issue 4
3 About This Code 4
4 16 Standards 5
4.1 Best interests of the child: 5
4.2 Age-appropriate application: 5
4.3 Transparency: 5
4.4 Detrimental use of data: 5
4.5 Policies and community standards: 5
4.6 Default settings: 6
4.7 Data minimisation: 6
4.8 Data sharing: 6
4.9 Geolocation: 6
4.10 Parental controls: 7
4.11 Profiling: 7
4.12 Nudge techniques: 7
4.13 Connected toys and devices: 7
4.14 Online tools: 7
4.15 Data protection impact assessments: 8
4.16 Governance and accountability: 8
5 Summary 8

A response to Age Appropriate Design: a code for online services

1 Outline

At **GDPR in Schools**, we have been working with our customers, the wider school community, IT Professionals, the DfE and the wider Information Governance / Privacy sector. We warmly receive the consultation document on Age Appropriate Design: a code of practice for online service.

There are many key areas that are being addressed by this code of practice that will benefit children and parents, and also provide online service providers with a healthy framework for managing their relationship with children and parents by doing the right thing.

Whilst the code is aimed at ISS who supply services directly to children, we do have to take into account the impact on schools. ICO guidance states, ***"If an ISS is only offered through an intermediary, such as a school, then it is not offered 'directly' to a child"*** and this code of practice clearly reflects that, touching very lightly on anything school related. The whole tone of the code is understandably geared towards the ISS provider being the data controller with a direct relationship with the data subject(s), whether directly or additionally via their parents. For the sake of ease, I will refer to this as 'home' to differentiate it from school.

This creates a dilemma in the approach to how providers who only work with schools, who have two streams of engagement (direct to home / direct to schools) or who have a blended approach involving both school and home. I will refer to the latter as 'blended'.

The direct relationship with home is being well addressed in the draft code. The 16 standards will form a core that all ISS services should uphold for all users, not just children but as company with experienced educators, school governors, providers of services to schools over many years, we fully appreciate and welcome the required focus on children. This was raised over 10 years ago when Becta reviewed guidance to suppliers of software handling / using data, and it is a shame it has taken so long to move onto the next steps. Some of our responses are based on needing to find a way to keep schools, or other affected institutes / organisations, involved either directly or indirectly in this code. As a result, there will be areas we outline as gaps which may not have been part of the original intent of the code but will hopefully provide beneficial information to either fit into the code or to have as guidance in addition to the code.

2 Key Issue

There are specific areas that could cause confusion and possible conflict between school and home, as well as making adherence to the code difficult for providers who offer to both or in a blended manner. A key issue, in fact it is the core element of this, is the judgement of who is the data controller. We still have examples of providers to schools who assert that they are the Data Controller, even to the point of they want to force schools to make sure all parents give **Consent** for their product to be used, whereas the school would operate under the lawful basis of **Public Task**. This clearly needs to be addressed within this guidance to ensure that no provider attempts to force consent.

3 About This Code

We have already outlined where this code doesn't address services which are then delivered via schools. A statement to outline this but to be mindful of the needs of schools and other affected institutes is important.

The code also states about how it supports parents / guardians, but schools have a duty to be informed and make informed decisions. There is a clear gap here.

4 16 Standards

Our response to the 16 standards is as follows:

4.1 Best interests of the child:

The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.

> This is to be done taking into account the needs of other stakeholders as they need to cover their own responsibilities, including as data controllers.

4.2 Age-appropriate application:

Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children.

> Age verification is generally managed by the schools themselves, but providers need to be mindful of schools differ in their approach to enabling access and use of applications. Some will have a walled garden approach where features are controlled to be suitable to age, yet others will not allow any access until they feel children have enough competence and understanding. Many parents will also want a similar approach, so this is beneficial to home, school and blended use anyway.

4.3 Transparency:

The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.

> Within schools, this will be provided by the schools themselves, but any assistance a provider can give is beneficial. Data Processing Agreements, contracts and T&Cs can be full of hard to digest information.

4.4 Detrimental use of data:

Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.

> As schools will be Data Controllers, the provider should only be doing what the school agrees or, where a blended approach is taken, any additional use should be part of an agreement between the school and the provider as Joint Data Controllers.

4.5 Policies and community standards:

Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).

> As schools will be Data Controllers, the provider should only be doing what the school agrees or, where a blended approach is taken, any additional use should be part of an agreement between the school and the provider as Joint Data Controllers.

4.6 Default settings:

Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

Settings will be determined by the school, but high privacy should be the default operated by the school anyway. Options for changing this must also be clear to the school to allow them to complete other tasks (see point 15)

4.7 Data minimisation:

Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

Providers will often provide schools with a list of data elements they require to deliver a service and explain how data will subsequently be processed. School will either agree that this is correct, they will set out a different set of data (and the provider can subsequently agree to provide a service based on this) or they will use a different provider. Ultimately the decision is with the school on what data is used to get a defined service.

4.8 Data sharing:

Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child. Age-appropriate design code.

As schools will be Data Controllers, the provider should only be doing what the school agrees or, where a blended approach is taken, any additional use should be part of an agreement between the school and the provider as Joint Data Controllers.

The code states ***"Data sharing can be done routinely (for example the provider of an educational app routinely sharing data with the child's school) or in response to a one off or emergency situation (for example sharing a child's personal data with the police for safeguarding reasons)"*** and this continues the thread that the provider is always the data controller. Without clear guidance within the code that a different situation applies within schools and other organisations, this will just repeat the mistake that the provider is the data controller.

Where a provider operates on behalf of the school to notify a 3rd party (e.g. a safeguarding / filtering provider who spots potential immediate suicide or self-harm messages may be tasked to inform relevant local support as agreed with the school) then this will also be reviewed as part of the DPIA (see section 15).

4.9 Geolocation:

Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session.

As schools will be Data Controllers, the provider should only be doing what the school agrees or, where a blended approach is taken, any additional use should be part of an agreement between the school and the provider as Joint Data Controllers. Schools have a responsibility to look at what is acceptable use of data and to ensure the purpose is both lawfully and ethically correct. See point 15.

4.10 Parental controls:

If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.

> An understanding of what controls schools may need is essential, and providers must be aware of the broad range of support and administration levels within a school. Where a provider operates a blended approach, there needs to be clear separation of controls for the home and school. The school already has a responsibility to inform children about how their data is used, so providers must be aware of possible areas of conflict when deciding to show children how data is used.

4.11 Profiling:

Switch options which use profiling off by default (unless you can demonstrate a compelling reason for profiling, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).

> As schools will be Data Controllers, the provider should only be doing what the school agrees or, where a blended approach is taken, any additional use should be part of an agreement between the school and the provider as Joint Data Controllers. Schools have a responsibility to look at what is acceptable use of data and to ensure the purpose is both lawfully and ethically correct. See point 15.

4.12 Nudge techniques:

Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off their privacy protections, or extend their use.

> Nudge techniques should not be used in any form for services to schools. Neither should children be able to change settings made by the school. Where a school requires engagement tools or personalisation tools, these should be clearly stated as such in the requirements from a school and within any DPA.

4.13 Connected toys and devices:

If you provide a connected toy or device ensure you include effective tools to enable compliance with this code.

> This is an increasing area for concern within schools. It is a growing trend to have smart speakers in administrative and classroom areas, with no or minimal thought given to data protection or privacy. All IoT devices should have high privacy by default and clear guidance on what information is recorded, shared and stored.

4.14 Online tools:

Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

> Historically there has been a raft of safeguarding initiatives that can be drawn on to support this work. Where services are provided to schools careful consideration is needed as to where reported concerns go to and where responsibility lies. Again, the role of Data Controller is a key issue here.

4.15 *Data protection impact assessments:*

Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

This is another important area to that underlines many of the standards mentioned above. Presently, we encourage providers to schools to draft DPIAs with key information about how their products work. The DfE presently has a work stream to support this activity as well. Through this code of practice, this can grow to be the norm, allowing schools to have a core framework to complete the DPIA based on their own individual needs and risks. Many schools do not fully know how software and services they use work and so additional guidance in this form would be a massive step forward. The needs of a school with MDM catering for vulnerable children on a 1-1 device scheme would assess the use of geolocation differently to that of a school where all devices remain in school and geolocating would help identify possible theft of devices. Context is key and providers can give schools a lot of help and support, but ultimately it is the school making the decisions (with variation for Joint Data Controllers).

4.16 *Governance and accountability:*

Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this code.

Data Processing Agreements between Data Controller and Data Processor are essential to allow schools to have a clear sight of how the provider supports them in their responsibilities. Ranging from breach notifications through to clarity of privacy settings. It is not just privacy notices to data subjects for the home scenario that need to be looked at, but more providers need to look at their data processing notices, contracts and T&Cs for greater clarity.

5 Summary

Whilst this draft is a significant step forward and will hopefully change the landscape of how children's data and privacy are respected, we must also be mindful of the other circumstances where children's data is used to provide services that might otherwise be considered ISS. This is especially relevant to those 'blended' circumstances.

We must also not be seen to put all the responsibility on the ISS provider in those circumstances, lest schools and other organisation incorrectly feel that it is not their responsibility anymore. Risk cannot be transferred completely from a Data Controller to a Data Processor. Rather than risk possible confusion, there is an opportunity to provide specific guidance to sit alongside the Code of Practice, benefiting both schools and their providers.

Work being done by ICO research grant holders around privacy and data protection needs to be included within this space as a well, combining efforts of DCMS (Online Harms) and others handling risks to children. A collected and consistent message is needed rather than dispirit messages from different providers.