| **Standard** | **Description**  | **Response** |
| --- | --- | --- |
| **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. | The service requires users to have restricted access to e-learning resources, which therefore requires user accounts. Additionally, it requires the ability to record the progress for the benefit of the school and the individual to assess their progress. This requires their personal information so that the school can identify each student’s progress and manage their accounts. |
| **Data protection impact assessments** | Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this code. | A DPIA has been undertaken, and this response to the AgeAppropriate Design Code incorporated. |
| **Age appropriate application** | Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead. | Resources are aimed at children 14-18 year olds and the process designed with that age range in mind. |
| **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. | Privacy policy is available with use of clear language with 14-18 year olds in mind. |
| **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. | Children’s personal data is not shared with third parties and is relied on purely to deliver the service. |
| **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). | Process in place to ensure that policy documents include the privacy policy and DPIA is reviewed annually.  |
| **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). | Current privacy settings are set at high, there is no reason to lower these privacy settings. Personal data is only processed for delivery of the service.  |
| **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. | Only minimal personal data required to deliver the service and required outcomes is collected. There are no nudging techniques for request of any additional data. |
| **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. | No Children’s personal data is shared with a Third party.  |
| **Geolocation** | Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). 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. | Geolocation is not used. |