Data Protection Impact Assessment

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	Name of school
Subject/title of DPIA	ARC Maths
Name of controller contact /DPO (delete as appropriate)	School contact

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
This is a new processing activity which processes personal data primarily of pupils but also of some school staff. All new projects involving the processing of personal data should have a DPIA performed, as recommended by the Information Commissioner's Office (ICO).

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Please see associated data flow diagram supplied by Arc Education. Pupils are prompted to supply a small set of personal data on first use of the ARC Maths app (name, school email address, school code, gender (M/F/not disclosed), MM/YY DOB and then proceed to complete the tasks/questions posed by. Their responses influence the nature of future questions posed to the individual pupil.

Pupils can view their progress on their dashboard, and school staff can view pupils' progress via their dashboard. Basic school contact data are collected to facilitate delivery of the app.

In the absence of any specific requests, pupils' personal data is retained for the default period of 18 months.

{school should add in any other processing activities outside of the ARC Maths app which form a part of the school process}

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Pupil data = name, school email address, school code, gender (M/F/not disclosed), MM/YY DOB, plus responses to the ARC Maths questions.

School Contact data = name, email address, telephone number, name of school, role in school.

No special category or criminal data is processed.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Data subjects are the school's pupils (primarily, plus a small number of staff). There are no explicit concerns regarding the nature of this processing which utilises a small data set, and is processed by a Data Processor (Arc Education (York) Ltd.) under the remit of a Data Processing Agreement with the school. The ARC Maths app has been positively assessed against the ICO's draft Age Appropriate Design Code (see associated document supplied by ARC Education) and both supports the aims of the code and represents a low risk to the data subjects.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
To improve educational outcomes for pupils in maths.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
{school should insert any consultation plans they have here, or state that as the processing is very low risk and high benefit there was no justification for additional consultation}. Arc Education, the Data Processor, have been consulted and supplied all appropriate documentations to ensure we meet the best interests of data subjects and are not exposing them to anything other than a low risk.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
{school would need to complete this – likely lawful basis of processing being necessary for the performance of a task in the public interest, i.e. improving educational outcomes for pupils in maths} ARC Maths has the ability to improve maths skills in its pupil users. The data collected is only available whilst using the app and cannot be shared with other processing activities – thus eliminating function creep. Only data which is adequate and required for the ARC Maths app to work effectively are collected, only the school email address is an acceptable email address from the pupil (thus protecting their interests in the event of an accidental data breach). Processing is under the authorization of a Data Processing Agreement with Arc Education. There are no international transfers to none-adequate nations (all data is held in the UK and EU).

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Disclosure of personal data – accidental breach of data resulting in disclosure of pupil's school email address, name, mm/yy dob and gender (if the pupil has submitted the gender data). The use of the school's email address is mandated and reinforced by the Data Processor who checks each new user again the domain of their email and the school code they submit (which identifies the school). Therefore pupils are protected by not having used their personal email address, thus reducing their exposure to spam/phishing attempts in the event of a breach. Developers are given access to live data to enable support however access to the data is strictly limited and password protected with an available record of access.	Remote	Minimal	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
n/a	n/a	n	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	School to complete this	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA