DPIA template

This template allows you to 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	Edward Williams
Subject/title of DPO	Managing Director
Name of controller contact /DPO (delete as appropriate)	Edward Williams

Step 1: Identify the need for a DPIA

Explain broadly what the 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.
Route-R synchronises with a school management information system to retrieve parent and pupil names, email and year to allow the parent and school to manage school bus bookings. Potentially medical records which are designed for teachers and support staff for less sensitive medical conditions such as allergies will be synchronized and available to bus drivers. Potentially absentee data will be synchronized to allow the system to remove passengers from the afternoon bus if they are absent.

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?
The source of the data is the school management information system and Route-R will have read only access to will not be able to add, edit or delete data. It is used to identify the parents and pupils to allow both parents and the school to manage bus bookings. The school bus team and drivers have access to the system. Drivers only have access to passenger lists. The driver requires access to the passenger list as they need to know who is on the bus and it is up to the school to ensure safe guarding measures are in place.

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?
The data is detailed in step 1. and as written, could include health data which is classes as special category data. No other categories are included or criminal data. Data is synchronized daily so it is only kept as long as present on the school management information system. Booking data is not deleted, this may be required by the school many years after a pupil has left the school and is compliant with GDPR. The data covers all school pupils wherever they live.

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)?
Our relationship is with the school not the parent or pupil and we have no direct contact with parents or pupils. Parents are able to login to their control panel and see their pupils listed and place, edit or remove bookings subject to the schools' terms and conditions. Our use of the data is open and expected. No data is passed to a third party. Data of pupils will always create a case for concern of security but we endeavor to code robustly using Microsoft Certified developers and best practice. Hacks of online data are possible to reported in the media from time to time and we continue to monitor potential approaches to access data without consent but we are not aware of any particular public concerns. We use graduates or higher who are Microsoft Certified but are not aware of a specific certified scheme.

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?
As covered in the previous steps, Route-R facilitates the management of the school bus, it improves safe guarding, reduces staff admin time and improves flexibility of bookings by parents.

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?
Parents can request the their personal details are removed by clicking a button within their portal but there is so little information there is very little we can consult on around personal data, we need what we have and cannot really offer the services without it, so they either use it or remove their details as they wish. We have no plans to consult other experts.

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?
The school must request and facilitate the synchronization, it is not possible without the school's permission and support. Route-R works and has achieved many successful journeys. There is almost always another way to achieve an objective but without the use of names and the ability to contact parents quickly and easily, particularly in the event of an emergency necessitates the data we hold. The data is synchronized with the school MIS system so data quality is outside Route-R's remit. Individuals have a portal and can see all of their data and bookings and we have supported their rights with the addition of the right to be forgotten button. We review our procedures regularly and at least annually and treat international transfer with the same, careful, approach.

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**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
System or database hacking	Possible	Minimal	Low
Parent portal hacking	Possible	Minimal	Low
Admin account hacking	Possible	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**
		Eliminated reduced accepted	Low medium high	Yes/no
System or database hacking	Check code, ensure server is patched, review code	Reduced	Low	Yes
Parent portal hacking	Ensure parents use strong passwords	Reduced	Low	Yes
Admin account hacking	Ensure admin use strong passwords	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Edward Williams/DPO/23/07/2019	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	N/A	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Edward Williams/DPO/23/07/2019	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:Ensure parent and admin use strong passwords. Note if using SSO this is outside Route-R's remit.		
DPO advice accepted or overruled by:	Ali Rizvi/Project Manager/23/07/2019	If overruled, you must explain your reasons
Comments: Task created, at least 8 characters long with a mix of numbers, special characters and letters with a mix of upper and lower case.		
Consultation responses reviewed by:	Edward Williams/DPO/23/07/2019	If your decision departs from individuals' views, you must explain your reasons
Comments: Approved		

This DPIA will kept under review by:	Edward Williams/DPO	The DPO should also review ongoing compliance with DPIA