DPIA: Staff Working Offsite During the Covid-19 Pandemic

This template follows best practice guidelines as an example of how schools and nurseries can record DPIA processes and outcomes. It follows the process set out in the ICO's DPIA guidance and should be read alongside the guidance criteria for an acceptable DPIA set out in European guidelines.

What is a DPIA?

A DPIA (Data Protection Impact Assessment) is a procedure designed to describe the processing of personal data. It assesses whether the processing is necessary and proportionate and helps to manage the risks to the rights and freedoms of the data subject.

Why do a DPIA?

Here's what you need to know:

- A DPIA is mandatory where processing is deemed to be 'high risk', or if your Data Protection Officer requests it
- It is good practice to conduct a DPIA for any new or existing major project which encompasses processing of large amounts of personal data
- The responsibility of carrying out a DPIA lies with the Data Controller, not the DPO
- If Controllers request it, Data Processors must assist with the DPIA
- If the conditions above are met, a DPIA must be done prior to processing personal data
- The DPO controls the overall process and structure of the data protection impact assessment
- The DPO must decide whether the data subjects need to be consulted when performing the DPIA
- In the case of a joint-controller relationship, each controller must define which part of the data processing activities belong to whom

Do not be frightened to engage in doing a DPIA. The outcomes and experience will enhance the overall ethos of an organisation's data protection philosophy. The benefits cannot be stressed enough.

Where to start in exceptional times!

This DPIA is like no other you will do as it is done at a time of crisis due to the Covid-19 pandemic. However, by carrying out this DPIA it will raise issues not yet thought of to ensure all your data continues to be safe when normal times have returned. Bringing awareness to your staff can only have a positive effect. Review regularly during these times of uncertainty.

DPIA Details

Project name	Staff working offsite as an emergency measure during the Covid-19 pandemic for Green Park Academy
Project description	A study of the increased risks to well established data protection protocols when the school staff are told they must work offsite as an emergency measure during the Covid-19 pandemic.
Brief reason(s) why a DPIA should be carried out	The school is aware that when student and staff personal data is taken off site and used in a different setting other than the school there is an increased risk that the data may be breached. Thus, by carrying out a DPIA, the school is looking for ways to reduce the risk of data breach and ensure all personal data is kept safe.
Lead DP person(s)	Patrick Taggart – p.taggart@romeromac.com Christina O'Neill – c.oneill@romeromac.com
DPO(s)	School DPO, Warwickshire Legal Services
Date started	19/03/2020
Date completed	TBC

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	This DPIA will review access control and the risks of the personal data being accessed by unauthorised persons whilst being used offsite during the Covid-19 pandemic. It will consider unauthorised access to personal data and suggest ways to reduce breaches
Summarise why you identified the need for a DPIA	The school has become aware that allowing staff to work offsite challenges to the integrity of its data protection policy

Step 2: Describe the Procedures

Describe what happens:	
Why do schools expose themselves to this risk?	Staff working offsite has become necessary due to emergency measures implemented during the Covid-19 pandemic and it is essential to support students to further their education
Is there any legal reason this must happen?	It is not known with such measures in place if there is a legal requirement for schools to do this. However, the school believes they have a moral duty to continue to offer a learning package for its students and support for its staff
What else?	Children must be kept gainfully occupied and not gather with others to spread the infection
What types of processing have been identified as likely high risk.	Teachers process thousands of pieces of personal data during their normal teaching day. Some of this will include special category data such as medical and ethnicity and religion Administration staff will be looking at new intake data as well as staff payroll and HR information

Describe the scope of the data that might be compromised:	
What is the nature of the data, and does it include special category or criminal offence data?	Present on school systems is every possible form of personal data including special category data
How much data do you collect and use?	The school will handle the personal data of approx. 565 students, and approx. 80 teaching and administration staff
Where will this be located	Electronic data will be stored on network which may be accessed remotely. In addition, stand-alone PCs and other devices will be used. Paper records may be taken or generated offsite
How many individuals are affected?	All students and staff
What geographical area does it cover?	The staff live within a [25 mile] radius of the school at Guys Cliffe Avenue Leamington Spa Warwickshire. CV32 6NB

Describe the context of the personal data stored:	
What is the nature of your relationship with the individuals?	Various combinations of relationships exist between school, student, employee, parents, leavers, sub-contract staff
How much control will they have?	The school will ensure the rights of the individuals are met at all times
Would they expect you to use their data in this way?	Yes
Do they include children or other vulnerable groups?	Yes
Are there prior concerns over this type of processing or security flaws?	No
Is it a different way of working in any way?	No
What is the current state of technology in this area?	The school ensures the highest technology is available for its given budget and appropriate for the process for data processed onsite, or through its networks. If it leaves this environment the school loses control
Are there any current issues of public concern that you should factor in, particularly in relationship to increased incidents in schools?	No

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?	All staff have been DBS checked, undergone safeguarding and data protection training

Describe the purposes of the processing	
What do you want to achieve?	To continue to offer students a place to learn, albeit in a virtual environment. It is essential that no personal data puts at risk the data subject
What is the intended effect on individuals?	To reduce the risk to minimum of data being accessed by an unauthorised person
What are the benefits of the processing for you, and more broadly?	To ensure the school meets its duty of care to its staff and students

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.	These emergency measures have been implemented very quickly and thus there has been no time to seek the views of stakeholders. However, this school uses best practice to ensure all understand the implications of what is done
Who else do you need to involve within your organisation?	The whole organisation must be involved
Do you need to ask your processors to assist?	Yes, we will seek assistance from any data processors that are included in events where staff access data remotely
Do you plan to consult information security experts, or any other experts?	Yes, wherever possible and if available, we follow guidelines and obtain advice from our local authority, the DfE, the ICO and GDPR in Schools Limited

Step 4: Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular:	
What is your lawful basis for processing?	The majority of our processing will be done under the public task umbrella
Does the processing actually achieve your purpose?	Yes
Is there another way to achieve the same outcome?	No, only teachers and staff know the needs of the learners and if required to work remotely, risks to personal data cannot be avoided
How will you prevent function creep? This means the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, which may lead to potential invasion of privacy	Unknown
How will you ensure data quality and data minimisation?	N/A
What information will you give individuals?	The school community will be informed of the key areas where possible risks may occur when working offsite. The SLT and ICT Manager will be available to offer advice and will have access to the school DPO
How will you help to support their rights?	To ensure rights are met, the data protection lead team will advise SLT of best practice and will be available for advice.
What measures do you take to ensure processors comply?	N/A
How do you safeguard any international transfers?	N/A

Step 5: Identify and Assess Risks

Describe source of risk and nature of potential impact on individuals:				
No	**Risk if paper or electronic systems containing personal data are accessed by unauthorised persons**	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1	Unencrypted devices used	Possible	Significant	High
2	Others having access to devices	Possible	Significant	High
3	Loss of device	Possible	Significant	High
4	Divulging personal data to others	Probable	Significant	High
5	Breaches not reported	Probable	Significant	High
6	Teachers' mark sheets and records	Possible	Minimal	Low
7	Safeguarding information	Probable	Severe	High
8	SEN and FSM data	Possible	Significant	High
9	Staff, parent and governor records	Possible	Significant	High
10	Paper or electronic storage mishandled	Probable	Severe	High

Step 6: Identify Measures to Reduce Risk

Identify additional measures to reduce or eliminate risks identified as medium or high risk in Step 5:				
Risk No	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure communicated**
1	Unencrypted devices used Staff will be instructed remotely how to check that their devices are safely encrypted. Most should be in today's technology	Reduced	Medium	Yes
2	Others having access to devices Staff will be advised how to protect the data they use from others who may use the same device	Reduced	Medium	Yes
3	Loss of device Staff will be aware of the dangers of losing devices. This message will be stressed further	Reduced	Low	Yes
4	Divulging personal data to others Staff should ONLY process minimum personal data. Name and class should be sufficient	Reduced	Low	Yes
5	Breaches not reported Staff will be reminded regularly to report breaches as they have been instructed	Reduced	Medium	Yes
6	Teachers' mark sheets and records These can be kept solely in a teacher's possession	Reduced	Low	Yes
7	Safeguarding information There is a risk if this data needs to be transmitted. Staff must take extra care and think twice before	Reduced	Medium	Yes

	transferring any data as such			
8	SEN and FSM data As 6	Reduced	Medium	Yes
9	Staff, governor and parent records As 6	Reduced	Medium	Yes
10	Paper or electronic storage mishandled Staff will be advised to only remove from site data which is essential. Whole data sets must not be removed	Reduced	Medium	Yes

Step 7: Sign Off and Record Outcomes

Item	Name/date	Notes
Measures approved by:	Head teacher and IEB	Actions will be integrated into schools processes and will be reviewed regularly.
Residual risks approved by:	N/A	N/A
DPO advice provided:	Hannah Clemons & Jason Tubbs	
Summary of DPO advice: The school is entering uncharted territory for which there has been no specific planning. However, all staff have had training in data protection and they will have access to further advice to help them. As a school we subscribe to the GDPRiS software and services and will have means to gain best practice advice which can be shared. The advice to staff is to think carefully when handling school data and to consider the consequences if that data fell into the wrong hands. We are well trained, we need to put that training into action.		
DPO advice accepted or overruled by:	DPO advice approved	Not overruled
Comments:		
Consultation responses reviewed by:	SLT who fully approved	
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA