Privacy impact assessment template

As part of schools' responsibility under the Data Protection Act (DPA) 1998, it is recommended that they consider conducting a privacy impact assessment (PIA). PIAs allow schools to identify privacy risks posed to individuals in certain situations, and establish effective control measures, ensuring they comply with the principles of the DPA and meet individuals' expectations of privacy. Conducting a PIA at an early stage ensures that measures are in place – reducing associated costs and damage to reputation which might otherwise occur.

This template provides a model PIA for schools to utilise in a variety of situations, e.g. if a new IT system for storing and accessing personal data has been installed, or where data is needed to be used for an unexpected or more intrusive purpose – these situations are usually referred to as 'projects'. As PIAs are flexible, schools should adapt this template, ensuring it meets their specific requirements and the questions are tailored to each individual project.

Last updated: 8 May 2017

Section A – PIA screening questions

This section of the PIA should be used to identify whether a PIA is necessary. If any of the questions are answered ‘Yes’, it is a clear indicator that a PIA should be completed. If you answer ‘No’ to any question, it should be clearly justified and evidenced as to why it is not applicable. These questions can also be used to clearly identify which potential risks are relevant and, therefore, contribute towards the structure of the PIA.

Question	Yes	No	Unsure	Comments
Will the project involve collecting new information about individuals?				
Will the project require individuals to provide information about themselves?				
Will information about individuals be disclosed to other individuals or organisations who have not previously held information about the individual?				
Is any information about individuals held for purposes it is not currently used for, or in a way it is not currently used?				
Will the project involve using a new technology that might be perceived as being intrusive to an individual’s privacy?				
Will the project result in any decisions or actions taken against individuals which may have a significant impact on them?				
Will any information about individuals raise privacy concerns, e.g. information they may wish to keep private, such as criminal information held on DBS certificates?				
Will the project require you to contact individuals in ways that they may find intrusive?				

The following three sections are designed to outline the specific need for the PIA, once it has been identified as necessary using the screening questions above. This section should provide clarity on what the project will involve, the information required and the practical steps that will be taken to identify any risks.

Section B – Identify the need

You should:

- **Explain what the project aims to achieve, and what the benefits will be to the school, to individuals and to other members of the school community.**
- **Summarise why the PIA was needed, in light of any questions that were answered 'Yes' within the 'PIA screening questions' section.**
- **Link to any other relevant documents related to the project, e.g. a project proposal.**

Section C – Provide the information flow

You should:

- **Describe the process for the collection and deletion of any personal data.**
- **Explain what information is used, what it is used for and who will have access to it.**
- **Detail how many individuals are likely to be affected by the project.**

It may be useful to detail the information flow using an Information Asset Register**.**

Section D – Practical steps

You should:

- **Explain what practical steps will be taken to ensure that all privacy risks are identified and addressed.**
- **Detail who will be consulted internally and externally, and how this consultation will take place.**

Section E – Identify the risks

This section should be used to identify the specific privacy risks to individuals involved within a project, as well as compliance risks in relation to the DPA and specific risks related to the school, e.g. reputational damage. All of these risks are usually overlapping – privacy risks to individuals may also lead to compliance risks, as well as risks to the school itself. Risks to individuals are categorised in many different ways, and it's important that all of these are considered and addressed – these can be related to physical safety, material damage, financial loss, or emotional distress. For each question, you should tick either 'Yes', 'No', or 'Unsure', then provide additional information for each question to justify and explain your answer in the comments box.

Risks to individuals and the school

Question	Yes	No	Unsure	Comments
Will there be adequate disclosure controls in place to decrease the likelihood of information being shared inappropriately?				
Will the context in which the information is used change over time, leading it to be used for a purpose that the individual may not be aware of?				
Will the project involve the introduction of any new surveillance methods?				

Could the measures used to gain information from the individual be perceived as intrusive in any way?				
Will data be shared and merged between the school and other organisations? Is the individual aware of which information may be accessed?				
Will the project involve gaining information from individuals which may prevent them from remaining unidentified?				
Are individuals aware of the risks of identification and disclosure of information?				
Will gaining information mean that the school is no longer using information which is safely anonymised?				
Are appropriate procedures in place to ensure that information is not collected and stored unnecessarily, including ensuring that duplicate records are not created?				
Has an appropriate retention period been established?				

Risks to compliance

	Question	Yes	No	Unsure	Comments
Principle 1 – personal data shall be processed fairly and lawfully	Have you identified the purpose of the project?				
	Is there a lawful reason you can carry out this project?				
	Have you identified the social need and aims of the project?				
	Are your actions a proportionate response to the social need?				
	Have you established a process for how you tell individuals about how their personal data is used and stored?				
	Do you need to amend your privacy notices?				
	Have you established which conditions for processing data apply to the project?				
	If sensitive personal data is involved, have you established which conditions for processing this data apply to the project?				
	If there is consent involved to use the personal data, is there an appropriate method in place for how this will be collected and what will be done if the data is withheld or withdrawn?				

	Will your actions interfere with the right to privacy, as outlined within the Human Rights Act 1998? If so, are the actions necessary and proportionate?				
Principle 2 – personal data shall only be obtained for one or more specified and lawful purposes	**Does the project plan cover all of the purposes for processing personal data?**				
	Is there any personal data that could not be used, without compromising the needs of the project?				
Principle 3 – personal data shall be adequate, relevant and not excessive	**Is the quality of the information sufficient enough for the purposes it will be used?**				
	Is there any personal data that could not be used, without compromising the needs of the project?				
Principle 4 – personal data shall be accurate and, where necessary, kept up-to-date	**If the procurement of new software is involved for the project, will it allow you to amend and delete information when necessary?**				
	Have you ensured that personal data obtained from individuals and/or other organisations is accurate?				

Principle 5 – personal data processed for a purpose shall not be held for longer than necessary	**Have you established a suitable retention period for the personal data you will be processing? (outline how long you will keep the data for)**				
	If you are procuring software, will this allow you to delete information in line with your retention periods?				
Principle 6 – personal data shall be processed in accordance with the rights of data subjects	**Do you have a process in place to respond to subject access requests?**				

Principle 7 – effective measures shall be taken against unlawful or unauthorised processing of data, and accidental loss, destruction of, and damage to, personal data.	**Do any new systems provide protection against the security risks you have identified?**				
	If the project involves a new system, are measures in place to ensure staff receive appropriate training and instruction, so they understand how to operate the new system correctly?				
	Have relevant staff received appropriate training and instruction relating to data protection and information sharing?				
Principle 8 – personal data shall not be transferred to a location outside of the European Economic Area (EEA) unless that location ensures an adequate level of protection	**Will the project require you to transfer data outside of the EEA? If yes, does the location ensure an appropriate level of protection?**				
	If data will be transferred outside of the EEA, are there appropriate measures in place to ensure that data is transferred securely?				

Section F − identify privacy issues and risks

This section should be used to identify each privacy issue, and outline how the issue will affect individuals, the school or compliance with the DPA – note that some privacy issues will not be applicable for all of these, and may only cause risk to one or two. Each privacy issue should be provided with a reference number.

Reference number	Privacy issue	Risk to individuals	Risk to compliance	Risk to school
1	Individuals are not clear on what the project involves	Individuals are not aware that their data is being processed, how, or for what purposes	Non-compliance with principle 1 of the DPA – data is not processed fairly and lawfully	1. May lead to public mistrust 2. May lead to a sanction imposed by the Information Commissioner's Office

Section G – Identify and approve the solutions

In this section, you should assign each identified risk with a risk rating for the likelihood of it occurring, and the impact it would have on individuals using a scale of 1 (very little or no risk/impact) – 5 (extreme risk/impact). You should describe the actions you suggest should be taken to address the identified risks, as well as any future steps which would be necessary for the risk to be managed effectively. It should also be clear who is responsible for approving each solution.

You should also outline whether you will accept, reduce or eliminate each risk. It is important to note that not every risk needs to be eliminated completely – a PIA seeks to reduce the impact of a risk to an appropriate level, whilst still allowing for the project to take place successfully. Where a risk has been accepted, you should explain the reasons for this.

Reference number	Risk(s) identified	Risk score		Solution(s)	Result – is the risk accepted, reduced or eliminated?	Evaluation – is the risk to individuals acceptable after implementing the identified solutions?	Approved by (name and job role)
		Likelihood	Impact				
1	• Individuals are not aware that their data is being processed, how, or for what purposes. • Non-compliance with principle 1 of the DPA – data is not processed fairly and lawfully. • May lead to public mistrust. • May lead to a sanction imposed by the Information Commissioner's Office.	5	5	• A communication plan will be developed to ensure compliance with principle 1 of the DPA. • Individuals will be assured that they will be provided with communication materials. • All relevant staff will be informed of the need to understand and distribute the communication materials.	Reduced	The risk is reduced to an acceptable level – the communication materials will ensure that all individuals are fully informed, and then the risk will be eliminated.	Joe Bloggs – headteacher

Section H – Integrate the PIA outcomes

Once risks and solutions have been identified, it is important that these are successfully integrated back into the overall plan for the project. This section should be used to identify who is responsible for actioning each solution and ensuring that the necessary action takes place. It is also important to identify who should be contacted for any future privacy concerns that may arise.

Using the same 1-5 scale as in section G, assign each action with an anticipated risk score in relation to the likelihood and impact of the risk occurring, once the action has taken place.

Reference number	Action to be taken	Date for action to be completed	Anticipated risk score following action		Responsibility for action (name and job role)	Current status
			Likelihood	Impact		
1	Communication plan and materials to be developed	10.05.2017	2	2	Joe Bloggs – headteacher	Meeting arranged with headteacher and school business manager to develop communication plan

Contact for future privacy concerns

Name	
Job role	
Email address	
Telephone number	

Last updated: 8 May 2017