GUIDANCE NOTE – DATA PROTECTION IMPACT ASSESSMENT (DPIA)

This guidance note accompanies the document "Data Protection Impact Assessment" and is designed to assist Schools in completing this record.

If you do have any questions about this document please let us know.

General

This is a standard document that can be used to carry out a risk assessment on data protection in the workplace.

Legal Position

Under the GDPR, DPIAs need to be used in certain circumstances including: -

- Carrying out systematic and extensive profiling with significant effects on individuals;
- Large scale use of sensitive data (such as medical or criminal record information);
- Public Monitoring.

There is no need to carry out DPIAs for technology already in place. However we would advise doing DPIAs for new technologies and softwares used regardless of whether they meet the criterion.

Why Carry Out DPIAs?

There are three main reasons for this: -

1) Because in certain circumstances, we are legally required to do so;
2) The GDPR expects organisations to show accountability to data protection and carry out a privacy by design approach. This means that we consider data protection at the outset rather than thinking about it when an issue arises. To ensure you have this approach, DPIAs can help us assess any risk to peoples personal data.
3) Because DPIAs can help us evidence compliance with the GDPR if asked by the ICO. So carrying out DPIAs as a matter of course can help us evidence a privacy by design approach.

Who Should Complete The Assessment?

This will normally be carried out by a staff member within the school who is either senior in the organisation (Headteacher, Business Manager) or the staff member responsible for implementing the new technology/software. It may in fact be a combination of the two to do this.

Once it is completed, we would advise running this past us as DPO before finalising the DPIA. This is because it is advised under GDPR to involve your DPO on completing the assessment. We can then review and determine whether anything is missing from the DPIA.

If this new software/technology/project would present a high risk to individuals and these risks cant be mitigated reasonably, then you may need to consult the ICO before

implementing this measure. We would suggest reverting to Judicium in the first instance for advice before consulting the ICO if you are unsure.

How To Complete The DPIA

Firstly to insert the name of the School, who carried out the assessment and when the DPO reviewed the DPIA.

Within the DPIA there are regular references to "Project/Technology/System" – do delete/amend this wording as applicable. Then to complete the boxes as suggested below.

Name Of Project/Technology/System

In this box to complete a summary of the software/technology being used (i.e. what it does and how it impacts on personal data).

Aims Of The Project/Technology/System

Set out here, what the aims of the project/technology/system are and what are the anticipated benefits to the school.

Use Of Personal Data

Set out here whether the project/technology/system involves the collection/use of personal data. If so, what data it collects, whether the data is particularly sensitive and whether any new data is collected as a result of the project/technology/system.

Reasons For Processing

Set out here the reasons the School are processing including any fair processing conditions (such as with consent of the individual, in order to comply with a contract, legal obligation, etc). This is in order to comply with principle 1 of the data protection principles set under GDPR.

Also set out whether you intend to use this information for the purpose it is currently used or in a way it is not currently used.

Impact On Personal Data

Set out here how the processing of personal data will be impacted by the use of this new technology/software/project. Such as how often you will be collecting data. How long you will keep it for. What individuals are affected.

Risks To Individuals

Set out here the risks to individuals including: -

- risks on privacy (such as intrusion)
- risks to the School such as compliance risks and costs
- risk to information being shared inappropriately
- risks to collection, storing, sharing data
- risks to vulnerable people/sensitive information

Also set out the level of risk (i.e. low, medium, high).

Will This Information Be Shared With Third Parties?

If the answer is "no", this is all that needs to be inserted.

If the answer is "yes", also detail here what third parties will receive their information, what information will be shared, the reasons those third parties will receive this information.

What Steps Will Be Taken To Protect The Data?

Outline here all the measures that will be taken to protect the information. For example: -

- any security measures
- whether there are agreements in place
- who has been consulted on on the project/technology/software
- steps taken to destroy data when no longer needed
- training and awareness raising amongst staff/other individuals
- anonymise information where applicable
- providing guidance to others
- transparency with individuals (such as allowing others to access their information)
- necessity of processing the information

If the information is particularly sensitive or if you share it with third parties then you should acknowledge this and set out what additional steps you are taking to protect sensitive information and ensuring third parties keep the information secure.

How Will The Project/Technology/System Protect Data?

Set out here the steps taken by the project/technology/system to protect date. Such as if you have an agreement in place with the provider, details of their security measures, etc.

Any Other Factors To Consider

This is to add any detail that may have been missed by the previous sections.

If there is anything to add make sure you provide sufficient detail here.

Compliance Statement

Not necessary but it is a good idea to insert a general compliance statement, setting out that impacts have been considered and the School are satisfied that proportionate measures have been put in place.

You could also set out any agreed actions here too.

Do complete the sections highlighted yellow before completing.

DPO Statement

I have also added a DPO statement for the DPO to complete to show they considered and are satisfied with the contents of the DPIA.

Retention and Review

Finally once completed and signed, do ensure that you retain this DPIA to evidence GDPR compliance to the ICO (and to governors).

You should then keep the DPIA under review (for example every year to two years) to ensure that the DPIA is being followed and doesn't impose any risks to individual data.