Data Privacy Impact Assessments (DPIA)

Guide to completing a DPIA

A DPIA is a process which helps an organisation to identify and reduce the privacy risks to individuals whose personal information is used in a project. The General Data Protection Regulation (GDPR) will make it a legal requirement to carry out a DPIA where the use of the personal information is likely to result in a **high** risk to the privacy of individuals.

Examples might include use of new technologies, including proposals to use cloud storage facilities for school information, use of software that uses details from the SIMS database, use of CCTV and biometrics, such as finger print scanning.

A DPIA can be used to help you to design more efficient and effective ways for handling personal data, minimise privacy risks to the individuals affected and financial and reputational impact of a data incident on the school.

This guide is intended to help you assess whether a DPIA is needed, identify levels of risk of personal data for your project and complete a DPIA report (where applicable), which will need to be agreed and approved by (complete as appropriate – Headteacher/Data Protection Officer).

When to carry out a DPIA

A DPIA should be completed when the project is likely to involve collection of personal data that may involve a high risk to the privacy of individuals. You should take into account the following when deciding whether a DPIA is necessary.

1. If personal data is not being collected or processed there is no need to do a DPIA.

2. Will the project involve the collection of new or different types of information about individuals? If personal information will be collected using new technology, or collection of a new type of special category data not collected before, you should carry out a DPIA. If you will be collecting large amounts of personal information to use in a way not previously used, you should complete a DPIA.

4. Any project involving monitoring of individuals, such as installation of new CCTV, should always require a DPIA as should any use of biometric technology.

When to start a DPIA

If you are thinking about starting a project or making changes to existing services/ systems, then you should consider whether a DPIA is necessary from an early stage.

A DPIA should be started at project initiation stage, continued throughout the life of the project and re-visited in each new project phase, for example, when you want to use the personal data for a new or additional purpose for the use of the data, or if you are collecting

new personal data. This should be proportionate to the level of special category data being collected or processed as a result of the project.

It is important to start at an early stage of the process to allow for time to resolve issues and mitigate for any risks identified, in order to avoid the difficulties of having to address these points late in the project when other decisions have already been made.

How to carry out a DPIA

Use the checklist below to help you decide whether the project involves privacy risks, identify what they are and work out what steps you will need to take to minimise those risks as far as possible.

When you have considered all of the risks, you should come to a conclusion about anything you can do to eliminate or minimise the risks you have identified. Some examples might include:-

- Minimising the risks of collecting too much personal information on CCTV by siting and angling the cameras so that they are focussed only on perhaps the car park rather than the entire school playground, or the entrance door, not into the school office.
- Checking the questions you have asked on a form before you send it out and ensuring that you really need all of the personal information you have requested
- If you need to store personal information on paper records ensuring that you keep them in a secure location which cannot be readily accessed by unauthorised individuals.
- If using a laptop in a classroom, make sure that staff are instructed to lock the screen if they leave it unattended for a while.

When you have recorded all of these points and how you will address the risks, you should get it signed off – either by the Data Protection Officer (or if the Data Protection Officer is completing the form, by the Headteacher) and keep a copy to refer back to for audit purposes and for updating if the project is changed or extended in future.

Completing a DPIA

When you have completed the DPIA, considered any risks and mitigated them wherever possible, the school will need to decide whether to accept any remaining risks. It is good practice to document what risks were identified, what steps were taken to minimise them and what risks were accepted.

You will also need to consider who should sign off the final DPIA – e.g. Headteacher, Data Protection Officer.

You can find more detailed guidance on conducting privacy impact assessments on the ICO's DPIA code of practice

https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

DPIA Checklist

Project name: …….

Brief description of project: ……..

1. What is the project for? What does it seek to achieve?
2. Will the project collect information about individuals e.g. students, parents, staff? If no personal information is collected, a DPIA will not be required.
3. What type of information will it collect? Will it be special category data? e.g. information about an individuals physical or mental health, social care details, details of criminal offences or allegations, or collecting large quantities of personal information? Any of these will raise the level of risk.
4. How will the information be collected? On paper forms? Electronically? Who will have access to this information? How will it be stored and kept secure?

5. How will pupils/staff /parents be made aware of how their personal information is being used? Will a privacy notice be provided? At the end of a paper form? By linking to the school website privacy notice? Does the privacy notice provide sufficient detail about the reasons for collecting the information and who it may be shared with?
6. Do you need consent from the individual to use the information? e.g. because special category data is being collected.
7. Does the project involve the use of new or different technology which could be privacy intrusive e.g. CCTV, monitoring of staff, biometrics, GPS tracking or cloud storage
8. What risks have been identified? What steps have been taken to eliminate or minimise them?
Signature: …….. Name (printed): ……. Position: …… (Headteacher or DPO) Date: ……..