Chalkhill Primary School

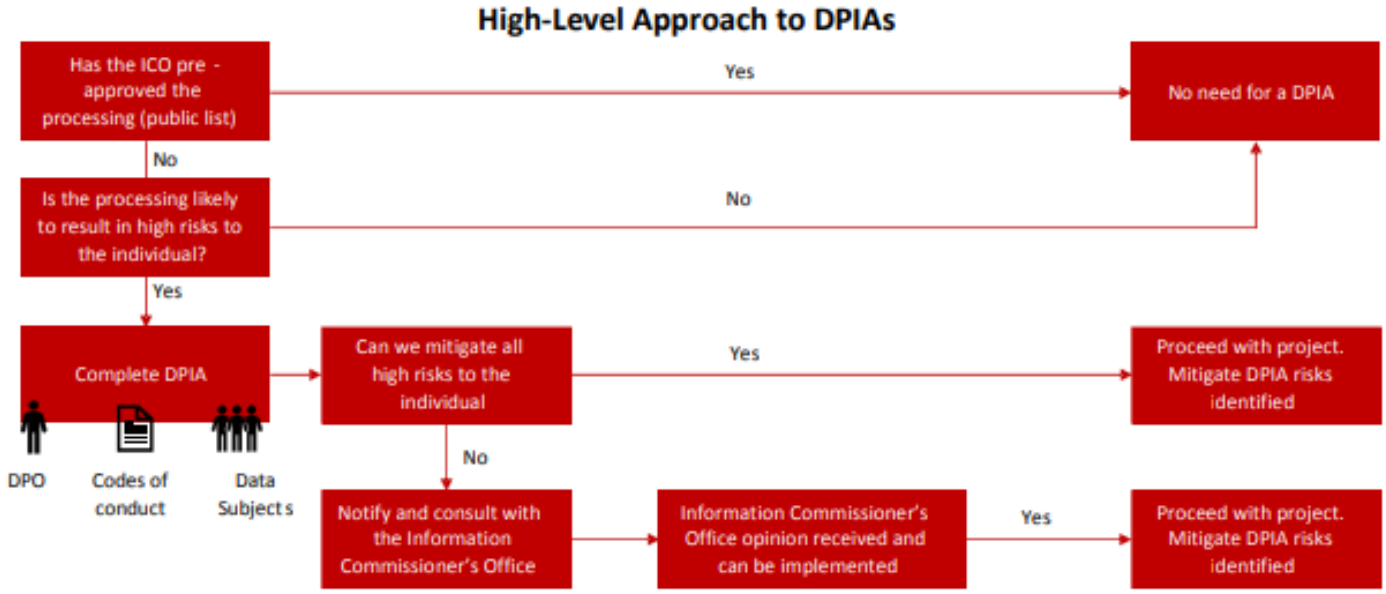
Data Protection Impact Assessment Policy and Procedure

Contents

Introduction 3
Has the ICO pre-approved processing 3
Evaluating what is a high-risk to the individual 3
Indictors that influence the DPIA decision (more detail in appendix 1) 4
Reliance on existing DPIAs 4
DPIA Process 4
Describing information flows 5
Identifying privacy and related risks 5
Identifying and evaluating privacy solutions 6
Signing off and recording the PIA outcomes 6
Integrating the PIA outcomes back into the project plan 6
Appendix 1: Indicators of High-Risk to the individual that may justify a DPIA 7

Introduction

A Data Protection Impact Assessment ("DPIA") is a process designed to describe the processing, assess the necessity and proportionality of that processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data. Chalkhill Primary School considers the need for a DPIA for all changes. We only complete a DPIA where there is likely to be a high risk to the rights and freedoms of the individual.



Has the ICO pre-approved processing?

The ICO may decide that certain activities such as the standard school application process does not require a DPIA. Where the ICO makes these decisions, we will not complete a formal DPIA. However, we will review the available information from the ICO to confirm that the decision applies and consider if we need to consider any activities we are completing which do not fall into the scope of the ICO decision.

Evaluating what is a high-risk to the individual

Chalkhill Primary School recognises that DPIA's are required in a limited number of cases. The GDPR requires a DPIA where the processing is likely to result in a high risk to the rights and freedoms of individuals. The GDPR highlights the following examples of processing that would require a DPIA:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10;

(c) a systematic monitoring of a publicly accessible area on a large scale. To determine if there is likely to be a high risk to individuals the DPLs will meet with the Data Protection Officer to discuss the project. At the meeting we will discuss the below 10 indicators of risk to assess the need for a DPIA. If two or more of the indicators are met by the processing the school will complete a DPIA. Note we do not consider the normal school activities of testing and evaluating pupils to require a DPIA.

Indictors that influence the DPIA decision (more detail in appendix 1)

1. Evaluating or scoring of individuals including profiling and predicting behaviour;

2. Automated decision making with legal or similar effect (unlikely to apply to the school);

3. Systemic monitoring of publicly accessible places;

4. Processing of sensitive data including, racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data for the purposes of identifying a person, health, sex life, sexual orientation;

5. Large scale data processing (unlikely to apply to the school);

6. Datasets that have been matched or combined;

7. Data concerning vulnerable data subjects (including children);

8. Innovative use of applying technology or organisational solutions;

9. Data transfers across borders outside of the EU;

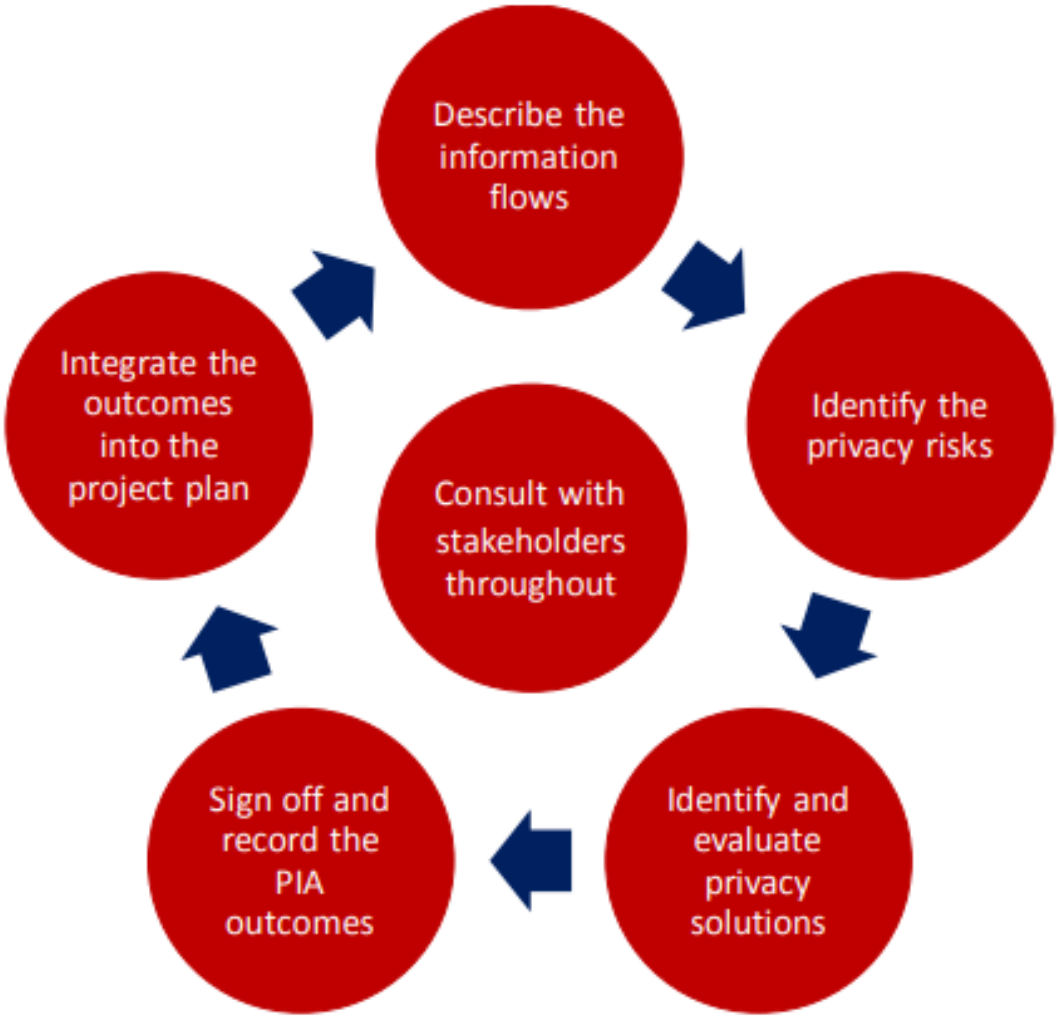
10. When processing limits the individual's rights.

Reliance on existing DPIAs

We can and will rely on existing DPIAs where they have already assessed the risks of similar processing, e.g. if we purchase an IT system that has been implemented in many schools we will ask the IT company to provide any existing DPIA. In addition, we will request DPIAs from other schools where this is appropriate and DPIAs exist.

DPIA Process

Where we decide a DPIA is required we will complete one as early as possible in the process and will update the DPIA at points in the project. The School is responsible for the DPIA. The DPO should be included as an advisor in the process. Where it is possible we will invite pupils, parents, and staff to participate in the DPIA to gather their views.



Describing information flows

• Explain how information will be obtained, used, and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.

• This process can help to identify potential 'function creep' - unforeseen or unintended uses of the data (for example data sharing)

- ✓ People who will be using the information are consulted on the practical implications.
- ✓ Potential future uses of information are identified, even if they are not immediately necessary.

Identifying privacy and related risks

• Record the risks to individuals, including possible intrusions on privacy where appropriate.

• Assess the corporate risks, including regulatory action, reputational damage, and loss of public trust. Conduct a compliance check against the GDPR and other relevant legislation.

• Maintain a record of the identified risks.

- ✓ The process helps the school to understand the likelihood and severity of privacy risks.
- ✓ The school is open with itself about risks and potential changes to a project.

Identifying and evaluating privacy solutions

• Devise ways to reduce or eliminate privacy risks.

• Assess the costs and benefits of each approach, looking at the impact on privacy and the effect on the project outcomes.

• Refer to the privacy risk register until satisfied with the overall privacy impact.

- ✓ The process considers the aims of the project and the impact on privacy.
- ✓ The process also records privacy risks which have been accepted as necessary for the project to continue.
- ✓

Signing off and recording the PIA outcomes

• Obtain appropriate signoff within the organisation.

• Produce a PIA report, drawing on material produced earlier during the PIA.

• Consider publishing the report or other relevant information about the process.

- ✓ The PIA is approved at a level appropriate to the project.
- ✓ A PIA report or summary is made available to the appropriate stakeholders.

Integrating the DPIA outcomes back into the project plan

• Ensure that the steps recommended by the DPIA are implemented.

• Continue to use the DPIA throughout the project lifecycle when appropriate.

- ✓ The implementation of privacy solutions is carried out and recorded.
- ✓ The DPIA is referred to if the project is reviewed or expanded in the future.

Appendix 1: Indicators of High-Risk to the individual that may justify a DPIA

1. Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements".

2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person". For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion.

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area". This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s).

4. Sensitive data: this includes special categories of data as defined in Article 9 (for example information about children's health), as well as personal data relating to criminal convictions or offences. This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by a natural person in the course of purely personal or household activity (such as cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features, and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be perceived as very intrusive.

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the following factors, in particular, should be considered when determining whether the processing is carried out on a large scale a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b. the volume of data and/or the range of different data items being processed; c. the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity.

6. Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. For example, children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data.

8. Innovative use or applying technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks.

9. Data transfer across borders outside the European Union (recital 116), taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers or the likelihood of transfers based on derogations for specific situations set forth by the GDPR.

10. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91). This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract.