THE PAINSLEY CATHOLIC ACADEMY

The Painsley Catholic Academy

Better Together

Data Protection

Impact Assessment Policy

Sept 2022-24

GDPR

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which will determine how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data. It will apply from 25 May 2018 to organisations that process or handle personal data, including schools.

Data Protection Impact Assessment

Data protection impact assessments (DPIAs) are a tool that can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage.

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, **a DPIA is a process for building and demonstrating compliance**.

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*"

When to do a DPIA

It is for data controllers to determine whether a DPIA is required. Where it isn't clear whether a DPIA is required, it is recommended that one should be carried out, as it is a useful tool to help controllers comply with data protection law.

The criteria to determine whether a DPIA is required is:

1. Evaluation or scoring
2. Automated decision making with legal or similar significant effect
3. Systematic monitoring
4. Sensitive data or data of a highly personal nature
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organisational solutions
9. When the processing in itself prevents data subjects from exercising a right or using a service or contract

A DPIA may concern a single data processing operation or a single DPIA could be used to assess multiple processing operations that are similar.

The Information Commissioner's Office (ICO) explains that you must carry out a DPIA when:

Using new technologies; and

The processing is likely to result in a high risk to the rights and freedoms of individuals

Processing that is likely to result in a high risk includes (but is not limited to):

Systematic and extensive processing activities, including profiling and where decisions have legal effects, or similarly significant effects, on individuals

Large-scale processing of special categories of data or personal data relating to criminal convictions or offences
Large-scale, systematic monitoring of public areas (such as CCTV)

The ICO suggests, for example, that you might do this where you've considered implementing a new web monitoring system in the classroom or sharing data with a local troubled families initiative.

The GDPR requires controllers to implement appropriate measures to ensure and be able to demonstrate compliance with the GDPR, taking into account among others the “the risks of varying likelihood and severity for the rights and freedoms of natural persons”. The obligation for controllers to conduct a DPIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks presented by the processing of personal data.

DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. The data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate. Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities.

In addition, as part of the accountability principle, every data controller “*shall maintain a record of processing activities under its responsibility*”.

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.

The data controller:
Is responsible for ensuring that the DPIA is carried out, although someone else inside or outside the organisation can do it
Must seek the advice of the data protection officer. This advice, and the decisions taken by the controller, should be documented within the DPIA
Must seek the views of data subjects or their representatives, where appropriate

Contents of a DPIA

The ICO, linked to above, says that a DPIA should include:
A description of the processing operations and purposes, including, where applicable, the legitimate interests pursued by the data controller
An assessment of the necessity and proportionality of the processing in relation to the purpose
An assessment of the risks to individuals
The measures in place to address risk, including security and to demonstrate that you comply

Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.

Criteria for an acceptable DPIA.

These are:

A systematic description of the processing is
provided Necessity and proportionality are assessed
Risks to the rights and freedoms of data subjects are
managed Interested parties are involved

Template

The template in Appendix 2 taken from the ICO's guidance includes the following 6 steps:

1. Identify the need for a PIA
2. Describe the information flows
3. Identify the privacy and related risks
4. Identify privacy solutions
5. Sign off and record the PIA outcomes
6. Integrate the PIA outcomes back into the project plan

Links with other policies

This policy is linked to all College policies that include the storage or processing of staff or student data or the implementation of new technologies/initiatives that are involved directly with the storage or processing of staff or student data, including

CCTV Policy
Communications Policy
Counter Fraud and Corruption Policy
Data Protection Policy
Safeguarding Policy
Medical Needs Policy
Personal Data Policy
This list is not exhaustive.

References

http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
The Key https://schoolleaders.thekeysupport.com/administration-and-management/record-keeping/data-protection/data-protection-impact-assessments/?marker=content-body
ICO https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Appendix 1

Privacy impact assessment screening questions

These questions are intended to help organisations decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method which fits more closely with the types of project you are likely to assess.

- Will the project involve the collection of new information about individuals? Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

Appendix 2

Privacy impact assessment template

Step one: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the DPIA process.

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Privacy issue	Risk to Individuals	Compliance Risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns