SAINT TEILO'S TENBY

YSGOL TEILO SANT

Privacy Impact Assessment

‘Learning to follow the right Path through care, love and respect in the Light of the Risen Christ.’

<u>Important Note</u>

This procedure document has been produced based on current General Data Protection Regulations (GDPR) information. As further updates are released this procedure may be updated to reflect the changes.

Version History			
Version	**Date**	**Detail**	**Author**
1.0	21/05/2020	Completed for distribution	Mr C. Amos

Privacy Impact Assessment Procedure for St Teilo's Catholic Primary School

1. Introduction

A privacy impact assessment (PIA) is a tool which can help **St Teilo's Catholic Primary Primary School** identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective PIA will allow **St Teilo's Catholic Primary School** to identify and fix problems at an early project stage, reducing the associated costs and damage to reputation which might otherwise occur.

This procedure explains the principles which form the basis for a PIA.

The main body of the procedure sets out the basic steps which the School should carry out during the assessment process.

Templates are at Annex A and B

2. What is a Privacy Impact Assessment (PIA)?

A PIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a PIA should be used throughout the development and implementation of the School's project.

A PIA will enable the School to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

3. When will a PIA be appropriate?

PIAs should be applied to all new projects, because this allows greater scope for influencing how the project will be implemented. A PIA can also be useful when planning changes to an existing system.

A PIA can also be used to review an existing system, but the School needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system. The main purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met.

Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

Conducting a PIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising. A PIA should be undertaken before a project is underway.

4. What is meant by Privacy?

Privacy, in its broadest sense, is about the right of an individual to be left alone.

It can take two main forms, and these can be subject to different types of intrusion:

- **Physical privacy** - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

- **Informational privacy** – the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages
.

5. Informational Privacy

This procedure is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information.

Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to someone where the person who it is about does not want them to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information.

Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a PIA should be a minimisation of privacy risk.

6. The Benefits of a PIA

The Information Commissioner's Office (ICO) promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits.

Whilst a PIA is not a legal requirement (except 'high risk processing i.e. safeguarding data), the ICO may often ask an organisation whether they have carried out a PIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with the DPA.

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within the School and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a PIA would be appropriate

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more schools seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of the school.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications.
- The collection of new data on an existing system.

7. PIA Procedure

The format for an initial PIA is at **Annex A.**

This review form is based on the eight Data Protection Principles described in Schedule 1 of the Data Protection Act.

In the event that a full PIA is deemed appropriate the format for this is at
Annex B.

8. Monitoring

The completed PIA should be submitted to the Governing Body for review and approval. The Governing Body will monitor implementation of actions identified in PIA's

Appendices

Appendix A

Privacy Impact Assessment (PIA) Initial Screening Form

Project name:		**Date:**
Brief project outline:		
Project Lead:		

PIA Screening Questions

These questions are intended to help the Authority decide whether a PIA is necessary. Answering ‘yes’ to any of these questions is an indication that a PIA would be a useful exercise.

Once completed please return to the Information Governance Team for review:

Question	**Yes/No (√)**		**Notes**
Will the project involve the collection of new information about individuals?	**Y**	**N**	
Will the project compel individuals to provide information about themselves?	**Y**	**N**	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	**Y**	**N**	
Are you using information about individuals for a purpose it is not currently used for, or in a way it isnot currently used?	**Y**	**N**	
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.	**Y**	**N**	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	**Y**	**N**	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example,	**Y**	**N**	

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?	**Y**	**N**	

DPO

IGT Use

Date:

Officer:

Appendix B

Privacy Impact Assessment (PIA)

Project name:		**Date:**
Brief project outline:		
Project Lead Officer:		

Step 1: Identify the need for a PIA:

Explain what the project aims to achieve, what the benefits will be to the Authority, 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 PIA was identified (this can draw on your answers to the PIA Initial Screening Questions)

Step 2: 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.

Step 3: Describe the information flows

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 PIA process.

Step 4: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. (Please refer to the 'PIA – Identifying Compliance Risks' to help identify the DPA related compliance risks):

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

Step 5: 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 6: Sign off and record the PIA outcomes

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

Risk	**Approved solution**	**Approved by**

Step 7: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes 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