We are a Christian school that serves a diverse community and works in partnership with parents to develop the whole child.

St. Luke's CEVA UK GDPR DPI Procedure

Adopted: Summer 2022 **Review date: Summer 2024**

Version	Date	Amendment Details	Author
0.1	Autumn 2022	First Draft	Matt Hipperson

Signoff :

Role	Name	Date
Chair of Governors		
Head Teacher		
School Business Manager		

Contents

1.0 Overview

Data Protection Impact Assessment (DPIA) is the term the UK General Data Protection Regulation (UK GDPR) utilises for the risk based approach and pre assessment for high risk processing.

DPIAs are a requirement of the UK GDPR and a tool that can assist those with data protection obligations in identifying risks associated with data processing and posed to data subjects. It enables a pre-emptive approach to assess the risks and apply corrective actions and mitigating controls before a breach occurs.

The overall aim of a DPIA is to apply solutions and mitigating actions where a processing activity is deemed likely to cause a high risk to one or more individuals. Action to mitigate risks are subsequently documented and implemented. If appropriate, mitigating actions are reassessed to ensure that the risk(s) has been eliminated or reduced to an acceptable level. The overall scope of the risk solutions is to either: -

- Transfer the risk to another party
- Tolerate the risk by acceptance
- Terminate the risk by not proceeding with the proposed change
- Treat the risk by implementing solutions to reduce likelihood or impact

Where a DPIA indicates that the processing involved will or is likely to, result in a high risk to an individual and it is not possible to mitigate the risk with appropriate measures or controls, the DPO will consult the Information Commissioner's Office (ICO) prior to the processing taking place.

2.0 Scope and Applicability

The School will give consideration for the need of a DPIA at the start of all new projects. This will form part of the planning and development process.

3.0 General Policy

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the School or any 3rd parties on behalf of the School. Where risks of processing are high, the School employs the use of DPIAs to assess the risk, the impact and the likelihood, and to document the origin, nature, and severity of that risk, along with the processing purpose, reasons and mitigating measures and/or proposed solutions.

3.1 Identify if a DPIA is required

A DPIA is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals. Therefore the majority of projects within the school will not require a full DPIA.

In particular, the UK GDPR specifies that a DPIA must be conducted if the School plans to…

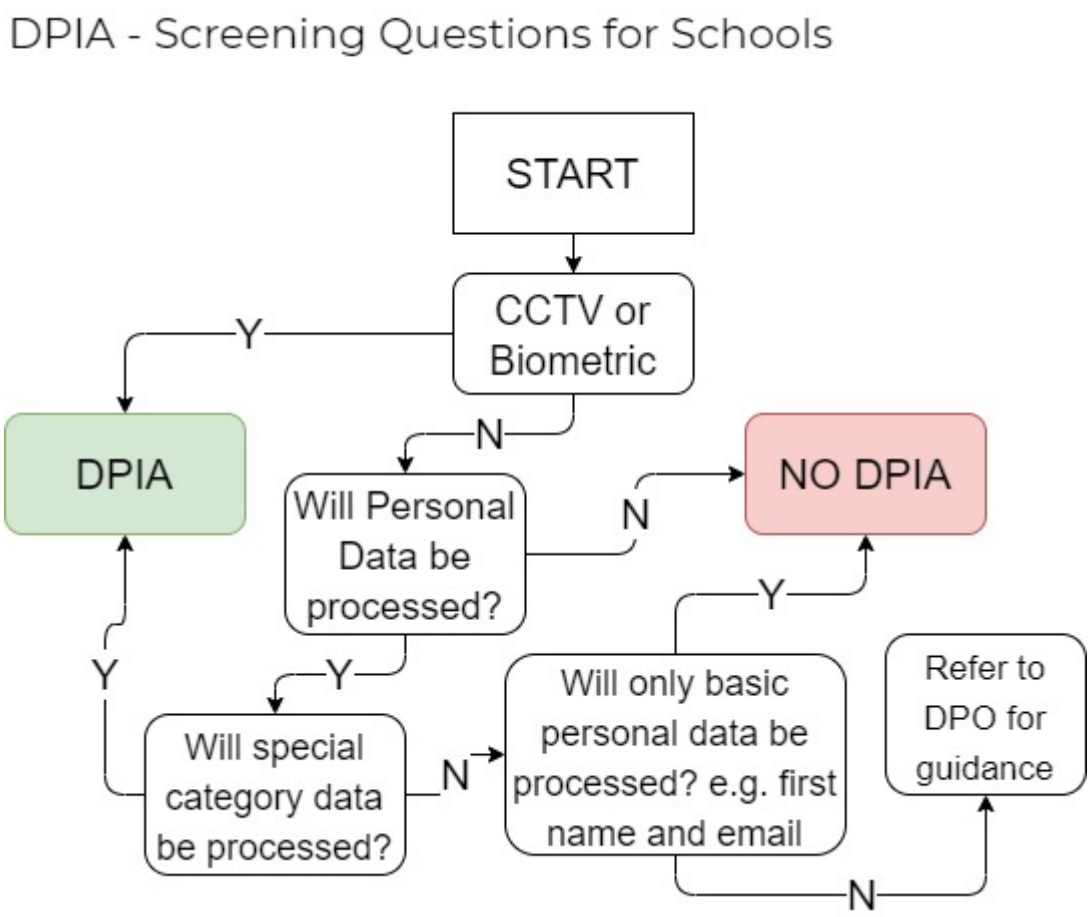
- Use systematic and extensive profiling with significant effects
- Process special category or criminal offence data on a large scale
- Systematically monitor publicly accessible places on a large scale

The ICO also requires a DPIA if the school plans to…

- Use new technologies
- Use profiling or special category data to decide on access to services

- Profile individuals on a large scale
- Process biometric data
- Process genetic data
- Match data or combine datasets from different sources
- Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')
- Track individuals' location or behaviour
- Profile children or target services at them
- Process data that might endanger the individual's physical health or safety in the event of a security breach

The school will utilise the following flow chart in order to determine if a DPIA is required.



The project lead will inform the DPO of any proposed changes which may result in the requirement for a DPIA. The project lead will provide sufficient information in order for the DPO to decide if a DPIA is necessary.

3.2 Completing the DPIA

The School will complete the DPIA Form with as much information as possible (Link - DPIA Template). The details required will include a description of the proposed project, its purpose and an assessment of the risks to the rights and freedoms of data subjects.

3.3 Risk Analysis

The DPO will review the DPIA Form provided by the School to undertake a risk assessment. Privacy issues and associated risks can be identified, judgement and reasoning will be used in order to assess both the likelihood and impact on personal data.

Once the risks have been identified, the risk matrix below will be used to identify a risk rating based on the impact and the likelihood of the risk occurring. This matrix provides a Red Amber Green (RAG) rating for how severe the risk could be to the privacy of individuals and therefore the necessity of implementing mitigating actions, or reassessing the project.

LIKELIHOOD	IMPACT					
		Trivial	Minor	Moderate	Major	Severe
	Almost Certain	Low Med	Medium	High	Very High	Very High
	Likely	Low	Low Med	Med High	High	Very High
	Possible	Low	Low Med	Medium	Med High	High
	Unlikely	Low	Low Med	Low Med	Medium	Med High
	Rare	Low	Low	Low Med	Medium	Medium
Impact x Likelihood = Risk						

- **Green** - Where an assessment outcome is Green, work should still be undertaken to see if the School can develop and implement any solutions or mitigating actions that can be applied to reduce the risk impact as far as possible. However, most green rated risks are acceptable and so focus should be placed on those with higher ratings.
- **Amber** - Where an assessment outcome is Amber, mitigating actions are always proposed and outcomes envisaged, before processing is approved. The aim is to reduce all risks down to a green (acceptable) level, however there will be occasions when processing must take place for legal/best interest reasons and so some processing with risks will go ahead and must be accepted into the project. All solutions and mitigating actions must first be considered, tried and applied if possible.
- **Red** - Where an assessment outcome is Red, it indicates that either or both impact and/or likelihood scores are unacceptable and that complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level. Some processing activities will be eliminated at this point as the impact to individuals is considered too high risk to proceed.

The outcomes will be recorded on the Schools risk register where applicable.

3.4 Evaluate DPIA

Where risks are identified, wherever possible consider action to mitigate the risk. It may not be possible to eliminate all risks. Where the School is unable to reduce risks to an acceptable level, a decision may be made to cancel the project. The aim is always to assess whether the impact on privacy is proportionate to the objectives of the project and to ensure that individuals and their privacy remain the priority.

The solutions will be recorded on the School's risk register where applicable.

The risk rating obtained in the evaluation process is used to ensure that the School is aware of any risks.

Steps which may be used to mitigate risks include…

- Changing the personal information collected to reduce the privacy level when processing
- Carrying out all processing in-house to avoid transfers or data sharing
- Utilising systems/technology to make the processing more accessible
- Creating new procedures for areas such as retention, destruction methods, exercising rights
- Developing new security measures for a specific project that align with acceptable levels of risk
- Ensuring that adequate and effective data protection training is provided to staff
- Publishing guidance manuals and supporting documents for use by those involved in the project
- Creating new materials and website content to enable better communication with individuals
- Carrying out a higher level of due diligence on any processors used for the project
- Producing data sharing agreements and data processing agreement

Costs and benefits associated with all solutions will be reviewed to ensure that they are viable, feasible and proportionate to the project impact. All solutions also involve a review and input from the DPO, who will review against current data protection legislation.

3.5 DPIA Outcomes

If a high risk is identified and the School wishes to proceed with the proposed change, the ICO will be consulted and advice should be received prior to the commencement of processing.

4.0 Roles and Responsibilities

The Head is responsible for involving the School's data compliance lead person at the start of any new project or major change to the School which involves personal data.

5.0 Compliance

Compliance is mandatory and will be enforced for all employees, vendors and contractors.

Non compliance with this and other School policies may be subject to disciplinary action, up to and including dismissal.

6.0 Risk Management

Risk management for the School is set out in the Risk Register.

7.0 References - none

8.0 Definitions

DPIA - Data Protection Impact Assessment

UK GDPR - The UK General Data Protection Regulation

ICO - Information Commissioner's Office

RAG - Red Amber Green

9.0 Review

This policy will be reviewed and updated on a regular basis, not to exceed 24 months.