Mission Statement
"A Caring Christian Family Where We Grow Together"

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

Effective Date: 16/03/2020 **Review Date: March 2025 Annual**

Review Date	Signed Executive Headteacher	Signed Director RCSAT
16/03/2020		
18/03/2021		
28/02/2022		
01/03/2023		
18/01/2024		

Persons Responsible for Policy:	Executive Headteacher RCSAT
Approval Date	16/03/2020
Signed:	Director RCSAT
Signed:	Executive Headteacher RCSAT

Introduction

The General Data Protection Regulation (UKGDPR) introduces a new obligation to undertake a Data Protection Impact Assessment (DPIA) before carrying out types of processing likely to result in 'high risk to individuals' interests', for example this could be the installation of CCTV cameras, the introduction of biometric technology or the purchase of a new management information system.

As a school you are unlikely to have to complete many DPIA's but, that just makes it all the more important to ensure you get it right when you do.

Put simply, a data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.

Effectively, it is evidence that you have considered all of the risks that may surround the project you plan to implement and that you have taken appropriate steps to deal with those risks.

You should complete the first part of the DPIA and pass it to us to review, we will then make a decision as to whether a full DPIA is required.

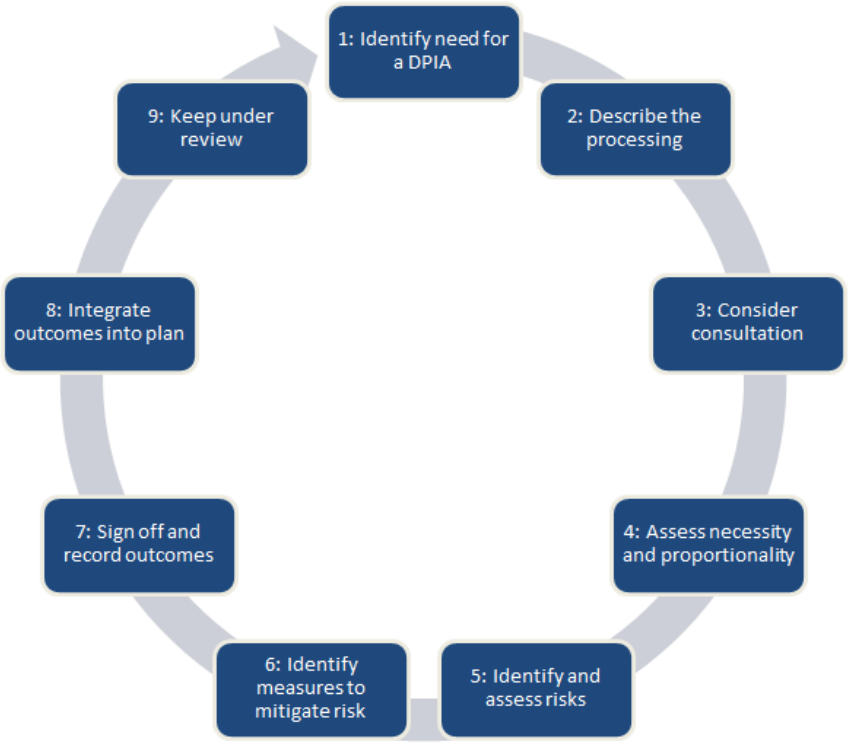
When to complete a DPIA

A DPIA is required if you are going to process personal data (e.g. collect, use, store, share or delete personal data), which could have a negative impact on people's rights and freedoms. It is particularly important to carry out a DPIA when you want to use new technology or process personal data in an innovative way, as this could increase the impact on the people involved.
You will need to carry out a DPIA in cases where the DPO considers your proposed activity is 'high risk' and could result in the following impact to individuals:

- they could suffer discrimination; identity theft or fraud; financial loss; reputational damage; physical harm or loss of confidentiality if a breach occurred;
- it will stop them from exercising their privacy or other legal rights;
- it will inhibit their ability to access services or opportunities;
- they could lose control over the use of their data;
- they will suffer significant economic or social disadvantage.

What activities could be 'high risk'?
There are several 'high risk' activities which schools carry out which are likely to require a DPIA. For example:

- Installing or upgrading CCTV on school premises.
- Purchasing a new system that will store personal data in the Cloud.
- Installing a visitor management system that will collect photographs and other personal data.
- Putting in place a system that will store lots of highly personal or sensitive data.
- Setting up employee remote access to the school's MIS and other systems.
- Implementing innovative technology which uses personal data e.g. technology which monitors or tracks students or employees.
- Collecting fingerprints to provide a cashless payment system or other uses of biometric data.
- Using radios in school for employees or students to communicate to one another.
- Publishing photographs and videos of children who are clearly identifiable.
- Setting up bulk or automated file deletion rules in email and other systems.
- Monitoring employees' or students' email or internet activity.
- Transferring large amounts of personal data from one system to another or regularly to a 3rd party.



When completing a DPIA, but in general you should identify, assess and document the following information:

- A description of the personal data you want to process and the reason why.
- A description of the measurers you will put in place to comply with the data protection principles.
- A description of the potential risks to individuals and an assessment of the impact of those risks.
- A description of the actions that will be taken to reduce the likelihood of the risks occurring.
- The remaining risk level after the actions will be put in place.
- Comments and recommendations made by the Data Protection Officer (DPO).
- Decision from senior management whether to go ahead with the proposed activity.
- Date when the DPIA should be reviewed by the DPO (e.g. annually or if any of the risks or actions change).

DPIAs should be carried out by someone with knowledge of the proposed activity and the potential impact it may have. Ideally, this should be a member of the Senior Leadership Team (SLT) in consultation with the IT lead where relevant. The Data Protection Lead should ensure an initial project assessment document is completed and sent to the DPO for assessment. The DPO will then decide if a full DPIA is required.
The DPO's advice is independent; their role is to advise when a DPIA is required and whether the activity will comply with data protection laws, privacy by design and general best practice.
The final decision to go ahead rests with the school's senior leadership, after careful consideration of the DPO's advice.

What are the potential risks?

There could be many different data protection risks associated with activities which you need to look out for. This will depend on what you intend to do with the data, but here are some examples of risk types:

- Unauthorised access to confidential or sensitive data.
- Where vital information cannot be accessed quickly due to IT failures.
- Unauthorised sharing or use of personal data.
- Data is accidentally lost or destroyed.
- Where inaccurate data could be used or shared.
- A system could be vulnerable to hacking or malicious activities.
- Covert monitoring could take place.
- Communications may be intercepted by unauthorised persons.
- Data is collected, used or shared without an appropriate legal basis.
- Individuals are not aware of how their data is being processed.
- Excessive information may be collected for the intended purpose.
- Data cannot be deleted from the system in line with retention schedules.

How can we reduce the likelihood of the risks occurring?

- Ensure everyone who handles personal data receives appropriate training, so they know how to access, use, share, store or destroy the data properly and in line with school policy.
- Restrict access to paper and electronic information only to those individuals who need access to it.
- Update your privacy notices to explain any new uses or sharing.
- Ensure there are robust IT security measures in place to defend against intruders, unauthorised modifications to the data and malicious software on your network.
- Identify the legal basis for processing the data with your Data Protection Officer.
- Use a system that enables data to be deleted or amended when required.
- Reduce the amount of data being processed or don't use identifiable personal data if it's not strictly needed.
- Encrypt portable equipment that contains personal data such as laptops and USBs.
- Carry out annual or more regular checks to ensure data is accurate and up to date.
- Don't allow the use of personal email address or equipment by members of staff or governors.

How do we decide if it's OK to go ahead?

As part of your assessment, you should evaluate and document what your risks and impacts are; the level of impact on the data subjects and the likelihood of the risks occurring; what actions you intend to take to reduce them and the final risk level after the actions have been applied.

The DPO will assess the level of impact, the likelihood of the risk and the risk level after any actions to reduce or eliminate the risk are put in place. A low assessment would mean that the proposed activity is unlikely to breach data protection legislation. If the risk is considered medium the DPO

will assess whether there is anything further that can be done to reduce the likelihood of a risk occurring. If the risk level cannot be reduced and remains high, the school will have to decide whether they believe the risk is acceptable.
If the final assessment comes out as High and you cannot put in place any other mitigations to reduce this rating, then your proposed activity should not go ahead unless this is approved by the Information Commissioner. The Data Protection Officer will seek approval from the ICO in such cases or advise what else you can do to reduce the risk to a low or medium level.

Completing the DPIA Template

To make things easier in developing your DPIA, we operate a two stage approach which allows us to review a proposed project and decide if a full DPIA is required.

The two stages are:-

Stage 1 –The school needs to complete the Stage 1 form that outlines details of the project and the personal data that would be involved. This is essentially a screening process to ensure you don't conduct a DPIA when one wouldn't be necessary, as well as acting as evidence that a DPIA has been considered.
Once you have completed Stage 1 you should return it to schooldpo@cheshirewestandchester.gov.uk for us to review and we will let you know if we need to proceed with Stage 2.
The Data Protection Officer (DPO) will then assess, log and provide a DPIA reference number for your records.
Stage 2 – If we confirm you do need to conduct a DPIA, you will be asked to begin completing the Stage 2 document for review. Once you have sent Stage2 to us to review, we will assess any identified privacy risks and your options to reduce the risks, adding appropriate comments and advice.
This advice should be reviewed by the school's SIRO/Head/Governors depending on how you operate.

If we identify significantly high risks that cannot be mitigated against, we have an obligation to refer the project details to the Information Commissioner's Office for review.

DPIAs are not one offs and they should be regularly reviewed to record any key changes to the project that may occur.