Guidance notes on completing the Data Protection Impact Assessment Template

Step 1: Identify the need for a DPIA

You should check whether your processing is on the list of types of processing which automatically require a DPIA. If it is not, you need to screen for other factors which might indicate that it is a type of processing which is likely to result in high risk.

Please refer to the following sections on the DPIA advice note:

'It is mandatory to undertake a DPIA if you plan to:' 'The ICO also requires you to do a DPIA if you plan to': and 'What other factors might indicate likely high risk?'

Step 2: Describe the processing

Describe how and why you plan to use the personal data. Your description must include "the nature, scope, context and purposes of the processing".

The **nature** of the processing is what you plan to do with the personal data. For example, how you will collect, use and store the data; who will have access to the data; who you will be sharing the data with; whether you use any external processors; retention periods; and security measures.

The **scope** of the processing is what the processing covers. For example, the nature, sensitivity, volume and variety of the data; the extent, frequency and duration of the processing; the number of data subjects involved; and the geographical area covered.

The **context** of the processing is the wider picture, including internal and external factors which might affect expectations or impact. For example, this may include the source of the data; the nature of your relationship with the individuals; the extent of control individuals have over their data and if the individuals are likely to expect the processing; the characteristics of the individuals (i.e. children or other vulnerable people); whether there are any prior concerns over this type of processing or security flaws and/ or any current issues of public concern; and whether you have considered and complied with relevant codes of practice.

The **purpose** of the processing is the reason why you want to process the personal data. For example, what you hope to achieve by processing; the intended outcome for individuals; and the benefits of processing for you and/ or society as a whole.

Step 3: Consultation process

You should seek the views of individuals or their representatives (i.e. pupils / parents or employees) unless there is a good reason not to.

You may also need to consult your DPO, where appropriate with data processors and other stakeholders such as IT/Security experts/ legal advisors as needed throughout the process.

If you decide that it is not appropriate to consult individuals then you should document and explain why. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If your DPIA decision is contradictory with the views of consulted parties, you should also document your reasons for reaching a different conclusion.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures; in particularly consider the lawful basis for processing; whether your plans will meet your intended outcome; and if there is an alternative way to meet your intended outcome.

You should also document answers to the relevant questions outlined in Step 4 of the DPIA template.

Step 5: Identify and assess risks

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – this includes physical, emotional or material harm/damage.

In particular consider whether the processing could result and/ or possibly contribute to:

●inability to exercise rights (including but not limited to privacy rights);

●inability to access services or opportunities;

●loss of control over the use of personal data;

●discrimination;

●identity theft or fraud;

●financial loss;

●reputational damage;

●physical harm;

●loss of confidentiality;

●reidentification of pseudonymised data; or

●any other significant economic or social disadvantage.

Also include both the sources and potential impact of any security risks – for example, unauthorised access to, loss or modification of personal data.

You may also want to consider your own risks, such as the impact of regulatory action, reputational damage or loss of public trust.

Bear in mind that you need to assess both the particular likelihood and severity of the possible risks, this will enable you to objectively assess whether the risk is a high risk.

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

The above matrix is an example of a structured approach to looking at risk. Your School/ Academy may use a different method that you can adapt for the same purpose.

Step 6: Identify measures to reduce risk

Identify measures you could take to reduce or eliminate risks which you identified as medium or high risk in step 5 above.

For example, measures to reduce or eliminate risks could include:

●deciding not to collect certain types of data;

●reducing the scope of the processing;

●reducing retention periods;

●taking additional technological security measures;

●training staff to ensure risks are anticipated and managed;

●anonymising or pseudonymising data where possible;

●writing internal guidance or processes to avoid risks;

●using a different technology;

●putting clear data sharing agreements into place;

●making changes to privacy notices;

●offering individuals the chance to opt out where appropriate; or

●implementing new systems to help individuals to exercise their rights.

Please note this is not an exhaustive list. You can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

Also record whether a residual risk and its level remains, in other words whether any risk remains after measures to reduce or eliminate risks have been applied.

Step 7: Sign off and record outcomes

You should record:

● what measures you plan to implement ;

● whether each risk has been eliminated, reduced, or accepted;

●the overall level of ‘residual risk’ after taking additional measures; and

●whether you need to consult the ICO.

Bear in mind that it may not always be possible to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the proposed processing and the difficulties of mitigation. However, if there is still a high risk, you must consult the ICO before you can go ahead with the processing.

As part of the sign-off process, you should seek advice from your DPO on whether the processing is compliant and can go ahead. If you decide not to follow your DPO's advice, you need to record your reasons.

If you have decided to depart from individuals' views, you must document this and explain your reasons for doing so.

Your Next Steps

Once completed, you must incorporate the DPIA outcomes into your processing plans. You need to ensure any action points the DPIA may have identified are undertaken.

As previously stated, a DPIA is not a one-off exercise it is an ongoing process which should be regularly reviewed and reassess if anything changes. For example, if you make any significant changes to how or why you process personal data, or to the amount of data you collect, or if a security flaw is identified.

If you have decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, you need to consult the ICO before you can go ahead with the processing. See the Advice Note on DPIA for more information on the ICO consultation process.

It is good practice to publish your DPIA to aid transparency and accountability. If you are concerned that publication might reveal commercially sensitive information, undermine security or cause other risks, you should consider whether you can redact (black out) or remove sensitive details, or publish a summary. As a Public Authority, your School/Academy need to consider its freedom of information obligations, as privacy impact assessments are included in the definition documents for publication schemes for many public authorities.