Guidance for Schools and Academy Trusts on Data Protection Impact Assessments

What is a Data Protection Impact Assessment (DPIA) and when is it needed?

1.1 A Data Protection Impact Assessment is a type of audit used to help assess privacy risks. The purpose is to describe the type of processing, assess its necessity and proportionality and help to manage any risks to data subjects. Under the GDPR, DPIAs are mandatory where the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*". Carrying out a DPIA is one of the ways a School or Trust can demonstrate compliance in accordance with the accountability principle in the General Data Protection Regulation ("GDPR").

1.2 While they can also be carried out in other situations, Schools / Trusts need to be able to evaluate when a DPIA is required. Failing to carry out a DPIA when one should be carried out, not carrying it out properly or failing to consult the ICO when required can result in sanctions being issued to the School / Trust, including the risk of significant fines. If it is unclear whether a DPIA is required, it is recommended that you undertake one to ensure that you are compliant. If you decide not to carry out a DPIA, you should keep records of your reasons and keep the processing activity under review to assess whether there are any changes to the risk which means that a DPIA is required at a later date.

1.3 As well as thinking about carrying out DPIAs, Schools and Trusts should also consider whether any existing processing activities require a DPIA to be carried out where there is likely to be a high risk to individuals. For example, the ICO's Code of Practice for surveillance cameras makes it clear that it is good practice to carry out a DPIA if you are using CCTV cameras. You do not need to do a DPIA if you have already considered the relevant risks and safeguards in another way, unless there has been a significant change to the nature, scope, context or purposes of the processing since that previous assessment.

1.4 Staff should be trained to understand the need to assess whether a DPIA is required at the early stages of a project involving personal data and must involve the DPO at an early stage so that he or she can provide support and advice. Advice from other experts and professionals should also be obtained where appropriate.

1.5 If the processing is being undertaken by a data processor (for example, a supplier or service provider who processes personal data on the instruction of the school), the processor should assist the School or Trust in carrying out the DPIA. The GDPR contract clauses that you are required to put in place with data processors should include this requirement.

1.6 The GDPR also requires the School to seek the views of data subjects or their representatives "where appropriate". This means that in some circumstances, it may be appropriate to carry out a consultation with the affected stakeholders, depending on the circumstances. If you decide not to consult the affected data subjects as part of your DPIA, you should keep records of your justification for not doing so. In addition, if your final decision goes against the views that come forward as a result of your consultation, you should keep records of the reasons for your decision.

1.7 A DPIA can be used to assess the risks relating to a single data processing operation or to assess multiple operations that are similar. They can also be used to assess the data protection impact of technology, such as hardware or software.

1.8 The GDPR says you must do a DPIA if you:

1.8.1 use systematic and extensive profiling with significant effects;

1.8.2 process special category or criminal offence data on a large scale; or

1.8.3 systematically monitor publicly accessible places on a large scale

However, the above list is not exhaustive.

1.9 The ICO also requires you to do a DPIA if you plan to:

1.9.1 use new technologies;

1.9.2 use profiling or special category data[1] to decide on access to services;

1.9.3 profile individuals on a large scale;

1.9.4 process biometric data (which lots of schools do for cashless catering or to allow pupils to access library services);

1.9.5 process genetic data;

1.9.6 match data or combine datasets from different sources;

1.9.7 collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

1.9.8 track individuals' location or behaviour;

1.9.9 profile children or target services at them; or

1.9.10 process data that might endanger the individual's physical health or safety in the event of a security breach.

1.10 The Article 29 working party of EU data protection authorities has published guidelines with nine criteria which may act as indicators of likely high risk processing:

1.10.1 evaluation or scoring;

1.10.2 automated decision-making with legal or similar significant effect;

1.10.3 systematic monitoring;

1.10.4 sensitive data or data of a highly personal nature;

1.10.5 data processed on a large scale;

[1] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

1.10.6 matching or combining datasets;

1.10.7 data concerning vulnerable data subjects;

1.10.8 innovative use or applying new technological or organisational solutions;

1.10.9 preventing data subjects from exercising a right or using a service or contract.

In most cases, a combination of two of these factors indicates the need for a DPIA. However, this is not a strict rule.

1.11 Schools and Trusts need to be particularly aware of the need to carry out a DPIA where the data subject is deemed to be vulnerable, for example, because of the power imbalance between the individuals and the organisation. Example of vulnerable data subjects include children and employees, so Schools and Trusts need to be particularly alert to the need to carry out a DPIA if there is likely to be a high risk to these stakeholders as a result of a processing activity.

1.12 Even if there is no specific indication of likely high risk, the ICO recommends that it is good practice to do a DPIA for any major new project involving the use of personal data.

1.13 If the outcome of a DPIA is that there is a high risk to individuals and you cannot identify any steps to reduce that risk, the School or Trust must consult the ICO before commencing the processing activity.

1.14 A DPIA assesses the impact of any proposed processing operation, for example the use of new technology, on the protection of personal data. A DPIA should be carried out before the processing of the personal data starts and then updated throughout the lifetime of any project. This is so that the DPIA can help to inform the decisions that are being made about the processing activities.

1.15 The content of a DPIA must include the following as a minimum:

1.15.1 a description of the processing activities and their purposes;

1.15.2 an assessment of the need for and the proportionality of the processing;

1.15.3 an assessment of the risks to the rights and freedoms of data subjects;

1.15.4 the measures envisaged to address the risks and demonstrate compliance with the GDPR.

1.16 It is not necessary to eliminate all risks but you do need to assess how you can minimise risks and assess whether any remaining risks are justified.

1.17 Risks to individuals might include the following non-exhaustive issues:

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

1.17.2 inability to access services or opportunities;

1.17.3 loss of control over the use of personal data;

1.17.4 discrimination;

1.17.5 identity theft or fraud;

1.17.6 financial loss;

1.17.7 reputational damage;

1.17.8 physical harm;

1.17.9 loss of confidentiality;

1.17.10 re-identification of pseudonymised data; or

1.17.11 any other significant economic or social disadvantage.

1.18 The DPIA must consider the likelihood and the severity of any impact on individuals and should look at risk based on the specific **nature, scope, context and purpose** of the processing. The ICO recommends that DPIAs, or at least a summary of them, are published, with sensitive details removed if necessary but this is not currently a legal requirement.

This overview is not intended to be an exhaustive statement of the law and should not be relied on as legal advice to be applied to any particular set of circumstances. Instead, it is intended to act as a brief introductory view of some of the legal considerations relevant to the subject in question

Checklist to help you to assess if a DPIA is needed.

Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, organisations need to be able to evaluate when a DPIA is required. The following checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

The ICO's draft guidance on DPIAs states, "…the important point here is not whether the processing is actually high risk or likely to result in harm – that is the job of the DPIA itself to assess in detail. Instead, the question is a more high-level screening test: are there features which point to the potential for high risk?"

The School / Trust's DPO must be involved in the process of assessing whether a DPIA is required. The answers below can be used to help inform a decision about whether to carry out a DPIA. If it is unclear if a DPIA is required for the processing activity, it is recommended that one is undertaken to ensure compliance and as a matter of good practice.

The checklist below is not exhaustive and is indicative of the circumstances when a DPIA may be needed, for example, in some circumstances a DPIA should be carried out if only one question is answered affirmatively and in others two or more affirmative answers may lead you to conclude that a DPIA is needed. It is up to the School / Trust to decide if the processing is likely to result in high risk taking into account the nature, scope, context and purposes of the processing

The definition of "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Criteria	**Answer**
What is the objective/intended outcome of the project?	
Is it a significant piece of work affecting how services/operations are currently provided?	
Who are the data subjects or who will be affected by the project?	
Will the project involve the collection of new information about people? (e.g. new identifiers or behavioural information relating to individuals?)	
Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?	
Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?	

Criteria	**Answer**
Is data being processed on a large scale (consider the number of data subjects concerned, the volume of data and/or the range of different data items being processed, the duration of the processing and the geographical extent of the processing)?	
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?	
Will personal information be transferred outside the EEA?	
Is information about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?	
Will information about pupils or other vulnerable persons (e.g. employees) be collected or otherwise processed?	
Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)	
Is monitoring or tracking or profiling of individuals taking place?	
Is data being used for automated decision making with legal or similar significant effect?	
Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)	
Is sensitive data being collected including:	
i. Race	
ii. Ethnic origin	
iii. Political opinions	
iv. Religious or philosophical beliefs	

Criteria	Answer
v. Trade union membership	
vi. Genetic data	
vii. Biometric data (including facial recognition)	
viii. Finger or palm print data	
ix. Health data	
x. Data about sex life or sexual orientation?	
Does the processing include personal data relating to criminal offences or prosecutions?	
Will the processing itself prevent data subjects from exercising a right or using a service or contract?	
Is the information about individuals of a kind likely to raise privacy concerns or is it information people would consider to be particularly private or confidential?	
Will the project require contact to be made with individuals in ways they may find intrusive?	
Does the project involve new or significantly changed handling of personal data about a large number of individuals?	
Could the processing endanger the individual's physical health or safety in the event of a security breach?	
Does the processing involve collecting personal data from a source other than the individual without providing them with a privacy notice?	
Are you considering a major project which will involve the use of personal data?	

Example DPIA

For an example of a DPIA template, please click here to see the template available on the ICO's website which, at the time of writing, is subject to consultation which is due to end on 13 April 2018: https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

It is possible that the ICO's sample DPIA may be subject to amendment. Schools and Trusts should therefore refer back to the ICO's website to ensure that you are using the most up to date document.

Criteria for an acceptable DPIA

It is not obligatory to use the ICO's template and you may wish to develop your own template as long as it covers the following key requirements[2].

1. A systematic description of the processing is provided:

1.1 nature, scope, context and purposes of the processing are taken into account;

1.2 personal data, recipients and period for which the personal data will be stored are recorded;

1.3 a functional description of the processing operation is provided;

1.4 the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;

1.5 compliance with approved codes of conduct is taken into account;

2. Necessity and proportionality are assessed:

2.1 measures envisaged to comply with the Regulation are determined, taking into account:

2.1.1 measures contributing to the proportionality and the necessity of the processing on the basis of:

2.1.1.1 specified, explicit and legitimate purpose(s);

2.1.1.2 lawfulness of processing;

2.1.1.3 adequate, relevant and limited to what is necessary data;

2.1.1.4 limited storage duration;

2.2 measures contributing to the rights of the data subjects:

2.2.1 information provided to the data subject;

2.2.2 right of access and to data portability;

[2] Taken from the WP29 criteria to assess whether or not a DPIA is sufficiently comprehensive.

2.2.3 right to rectification and to erasure;

2.2.4 right to object and to restriction of processing;

2.2.5 relationships with processors;

2.2.6 safeguards surrounding international transfer(s);

2.2.7 prior consultation.

3. Risks to the rights and freedoms of data subjects are managed:

3.1 origin, nature, particularity and severity of the risks are appreciated or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:

3.1.1 risks sources are taken into account;

3.1.2 potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;

3.1.3 threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;

3.1.4 likelihood and severity are estimated;

3.1.5 measures envisaged to treat those risks are determined;

4. Interested parties are involved:

4.1 the advice of the DPO is sought;

4.2 the views of data subjects or their representatives are sought, where appropriate.