Data Protection Impact Assessment

When considering a purchase of a new service or product that involves processing personal data a DPIA will be conducted. The specific responsibility for this will be a named member of staff depending on the nature of the product. It is likely that each DPIA will require input from a range of individuals. The DPO role for each DPIA needs to be set out depending if their involvement is direct or supervisory. It is necessary to ensure appropriate controls are implemented to mitigate any risks identified on a case by case basis before a decision to proceed can be made.

The relevant member of the team will need to determine if there is a need for a DPIA at the start of each project. This will need to be assessed and take into account the nature of the proposed purchase, the aims and type of personal data involved. If the risk assessment suggests that the processing may result in high-risk it is necessary for the DPO to consult with the Information Commissioner before implementation. It is hard to conceive of an instance where it would be applicable in a school situation, but the staff must be aware that this is a possibility. A good DPIA is part of good procurement practice. DfE provide advice about Procurement in schools that can be accessed here https://www.gov.uk/guidance/buying-for-schools

Useful Screening Questions:

1. Will the project involve the collection of new information about individuals?
2. Will the project compel individuals to provide information about themselves?
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
5. Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
6. Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
8. Will the project require you to contact individuals in ways that they may find intrusive?

Impact Assessment Template

1. Identify the need for an Impact Assessment

2. Describe the information flows
   You should describe the collection, use and deletion of personal data.
   Identifying how many different members of staff will have access to the data

3. Consultation Requirements
   What practical steps you will take to ensure that you identify and address privacy risks

4. Identify the privacy risks for data subject(s)

5. Privacy Solutions
   How can you reduce any risks. Include how you will test they are working effectively

6. Complete the Assessment
   Sign off the assessment and conclude with a final decision regarding the new product

7. Include the assessment in the plan for implementing the new product/service.
   Are there any privacy concerns?

Does the product/service comply with the Data Protection Principles?

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- Have you identified the purpose of the project?
- How will you tell individuals about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- If your organisation is subject to the Human Rights Act, you also need to consider:
- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

Principle 2: Personal data shall be obtained only for one or more specified and lawful purposes

and shall not be further processed in any manner incompatible with that or those purposes.

- Does your project plan cover all of the purposes for processing personal data?
- Have you identified potential new purposes as the scope of the project expands?

Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Is the quality of the information good enough for the purposes it is used?
- Which personal data could you not use, without compromising the needs of the project?

Principle 4: Personal data shall be accurate and, where necessary, kept up to date.

- If you are procuring new software does it allow you to amend data when necessary?
- How are you ensuring that personal data obtained is accurate?

Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

- What retention periods are suitable for the personal data you will be processing?
- Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6: Personal data shall be processed in accordance with the rights of data subjects.

- Will the systems you are putting in place allow you to respond to subject access requests more easily?
- If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Do any new systems provide protection against the security risks you have identified?
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require you to transfer data outside of the EEA?
- If you will be making transfers, how will you ensure that the data is adequately protected?