KINGSTONE ACADEMY TRUST

APPROVED DOCUMENT

Data Protection Impact Assessment Policy	
Relevant School/s:	**KHS and KTPS**
Policy Officer:	**HY Professional Services**
Approval:	**Delegated**
Date of Review:	**January 2025**
Next Review:	**2 years / change in legislation**

Contents

Introduction

1. Kingstone Academy Trust] ("the Trust" / "we" / "us" / "our") processes a significant amount of personal information about its pupils, parents, staff, volunteers and other individuals that it comes into contact with. This can include sensitive information ("special category data").

2. Where a type of personal data processing is likely to result in a high risk to the rights of individuals, the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ("GDPR") requires that we must carry out a Data Protection Impact Assessment ("DPIA"). A DPIA is a form of risk assessment which is designed to help us identify data protection risks associated with a particular system, project or plan and to put in place measures to mitigate those risks.

The procedure

3. Our Procedure is designed to be user friendly and easy to follow for those tasked with undertaking the requirements of this Policy. There are 6 specific stages which are as follows:

    (1) Identify the need for a DPIA
    (2) Describe the processing
    (3) Assess necessity and proportionality
    (4) Identify and assess risks
    (5) Identify measures to mitigate the risks
    (6) Sign off and record outcomes

4. Each of these steps is set out below.

Step 1: Identify the need for a DPIA

5. The first step is to consider whether a DPIA is necessary. A DPIA will be necessary

where a data processing activity is likely to result in a high risk to individuals such as pupils, staff, parents, and others who we may come into contact.

6. Whether a data protection impact assessment is necessary or not, it is good practice to undertake one. A non-exhaustive list of examples when the Trust will undertake a DPIA include when we decide to introduce any of the following: -

    a. Central management systems such as SIMS, Arbor or BromCom
    b. Safeguarding Systems such as MyConcern or CPOMS
    c. School communications applications
    d. HR systems
    e. Cashless catering systems
    f. Other systems that require the use of biometric data
    g. When CCTV systems are implemented

7. If we decide that a DPIA is needed, the DPIA should begin at the project's outset before processing starts. The DPIA must then run alongside the planning and development process. A good analogy for comparative purposes is a school trip; when a school trip is planned, a risk assessment will always be undertaken before the trip takes place, and is kept under review as appropriate. Data protection requires similar care and attention before processing takes place.

8. Having identified the need to undertake a DPIA, the Data Protection Impact Assessment template should be completed following the guidance steps below.

Step 2: Describe the processing

9. Step 2 requires you to describe the processing. To do this, you will describe the **nature**, **scope**, **context,** and **purposes** of the processing.

10. The **nature** of the processing is what we plan to do with the personal data. You will be required to consider and answer the following questions:-

a. how do we collect the data?
b. where will the data be stored?
c. how will we use the data?
d. who has access to the data?
e. who will we share the data with?
g. how will the data be kept secure?
h. are we are using any new technologies
i. are we are using any novel types of processing?

11. The **scope** of the processing is what the processing covers. You will be required to consider and answer the following questions:-

    a. what is the nature of the personal data?
    b. what is the volume and variety of the personal data?
    c. what is the sensitivity of the personal data?
    d. what is the extent and frequency of the processing?
    e. what is the duration of the processing?
    f. how many data subjects are involved?
    g. what is the geographical area covered?

12. The **context** of the processing is the wider picture, including internal and external factors which might affect expectations or impact. You will be required to consider and answer the following questions:-

    a. what is the nature of our relationship with the individuals?
    b. do they include children or other vulnerable groups?
    c. how much control will they have over the processing?
    d. would they expect you to use their data in this way?
    e. have there been prior concerns or previous security flaws to do with this type of processing?
    f. is it novel in any way? Are there any current issues of public concern?

13. The **purpose** of the processing is the reason why we want to process the personal data. You will be required to consider and answer the following questions:-

a. what do you want to achieve?
b. what is the intended effect on individuals?
c. what are the benefits of the processing for you, and more broadly?

Step 3: Assess necessity and proportionality

14. Step 3 requires you consider the **necessity and proportionality** of the processing. In this regard, we are thinking about whether we need to process the data, and if so, is the proposed way of achieving it proportionate. You will be required to consider and answer the following questions:-

    a. what is the lawful basis for processing the data in this way?
    b. does the processing actually achieve the purpose?
    c. is there a less intrusive way to achieve the same outcome?
    d. how will we ensure the data is good quality and limited to what is necessary?
    e. what information will we give individuals about how their data is used?
    f. how will we help to support their rights under the GDPR?
    g. what measures do we take to ensure processors and other third parties comply with data protection law?
    h. how do we safeguard any international transfers of the data?

15. Some aspects of this section raise more complex questions of data protection law, particularly (a), (g) and (f). The DPO will be able to provide advice in responding to these questions.

Step 4: Identify and assess risks

16. Step 4 requires you to **identify and assess risks** associated with the processing. These risks should have become more obvious when completing the DPIA. However, there may be other risks that have not been identified, and which the DPO may raise when providing advice on the DPIA.

17. To assess whether the risk is a high risk, you will need to consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm may still count as high risk.

18. You should make an objective assessment of the risks by using the matrix below which enable you to think about the likelihood of harm and severity of risks:

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		

Step 5: Identify measures to mitigate the risks

19. Against each risk identified, you will need to consider **measures to mitigate the risks**. For example, you may consider:

    a. deciding not to collect certain types of data;
    b. reducing the scope of the processing;
    c. reducing retention periods;

d. taking additional technological security measures;
e. training staff to ensure risks are anticipated and managed;
f. anonymising or pseudonymising data where possible;
g. writing internal guidance or processes to avoid risks;
h. using a different technology;
i. putting clear data-sharing agreements with other data controllers into place;
j. making changes to privacy notices;
k. obtaining data subjects' consent to the processing of their data where appropriate;
l. implementing new systems to help individuals to exercise their rights; or
m. Selecting data processors who will provide a greater degree of security and ensuring that data processing agreements are compliant with the GDPR.

20. You should obtain the advice of the DPO as part of this aspect of the process.

21. We will not start high-risk processing until the appropriate mitigating measures are in place following the DPIA.

Step 6: Sign off and record outcomes

22. The DPIA will be signed off by a senior member of staff at the Trust, for example the head of the department to which the processing activity most closely relates.

23. As part of the sign-off process, we will seek and document advice from our DPO on whether the processing is compliant and can go ahead. If we decide not to follow our DPO's advice, we will record our reasons.

Post-procedure steps

24. We will integrate the outcomes of our DPIA into our project plans. We will identify any action points and who is responsible for implementing them.
25. We will monitor the ongoing performance of the DPIA.