Data Protection Impact Assessment (DPIA)

DPIA in relation to:
Implementation and ongoing use of an educational app that tracks student behaviour and safeguarding information - CPOMS. The information is held securely at an address shared with staff members only and is password protected. Access to CPOMS is managed by the school Designated Safeguarding Lead and Head Teacher.
Name and Position of Individual(s) responsible for DPIA:
Sarah Rayson Head Teacher
Assessment date: Dec 2023
Review date: Dec 2024 with regular review as needed prior to that date

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal.

Summarise why you identified the need for a DPIA.

You need to check whether your processing is on the list of types of processing which automatically require a DPIA. If 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.

The aim of using CPOMS.

We aim to use an educational app, CPOMS, in order to track student behavior and safeguarding information electronically. In particular, we seek to use this application to hold, track and analyse important safeguarding information for the children in our school and where necessary due to impact on the child/ren their families as well as to track and subsequently improve behaviour of students that are disengaged in school or exhibit challenging behaviour, parental contact.

The benefits of using CPOMS

We believe that the school, students and their parents will benefit from the use of this educational app in a number of ways:

- Moving to an electronic system for tracking behavior will enable the school to further its goal of reducing its use of paper.

- Tracking student behavior electronically will allow staff and the senior leadership team to more efficiently share information about a student's behavior and as a result, the process for identifying students that require more attention and subsequently assisting them, will be more streamlined. This will enable staff and senior leaders to utilise more of their time on other important tasks.

- The use of this application will allow staff to more easily analyse student behavioral trends and subsequently relay this information to parents at parents' evenings and in student reports. Therefore, the use of this application will facilitate improved reporting of student behavior to parents.

- Tracking safeguarding information and concerns electronically will allow staff, Designated Safeguarding Leads and the senior leadership team to more efficiently share information about safeguarding fulfilling our duty under KCSIE 2023 (Keeping Children Safe in Education Sept 2023) and as a result, the process for identifying students that require more attention and subsequently assisting them, will be more streamlined and efficient.

- The use of this application will allow staff to more easily analyse and respond to safeguarding trends and areas of concern, to subsequently relay this information to parents and appropriate external agencies as needed. Therefore, the use of this application will facilitate improved safeguarding procedures.

Why do we need to do a DPIA?

We have determined that a DPIA is required because it involves the tracking of individual's behaviour and safeguarding information. This is highly personal information and it relates to vulnerable data subjects, namely children. Processing of special category data at a large scale can be involved – a high volume of safeguarding information.

Step 2: Describe the processing

Describe the nature of the processing:

How will you collect, use, store and delete data? You might find it useful to refer to a flow diagram or other way of describing data flows.

What is the source of the data?

Will you be sharing data with anyone?

What types of processing identified as likely high risk are involved?

https://www.cpoms.co.uk/privacy/

Collection

Information relating to student behaviour is extracted from our school's Management Information System (MIS). The data is then securely uploaded to CPOMS, using industry standard SSL/TLS encryption. CPOMS would disclose your Information if required to do so by law, for example, under a court order.

Usage

Information is used to track student behaviour and safeguarding concerns and subsequently measure whether certain student/ safeguarding outcomes have been achieved. CPOMS also produce customised reports on request by staff users. This outlines the progress of pupils on the programme and highlights key outcomes/ safeguarding concerns/ meeting outcomes/ SEN information produced.

Storage

Information is retained for the duration of the school's relationship with CPOMS or in the case of a particular child's information, information is archived when a child leaves the school or transferred securely online if the receiving school is also a CPOMS school. CPOMS use Microsoft and other IT service providers to process and store Information but, otherwise, we do not share your Information with any other external organisations.

Information may be stored and processed by CPOMS or by our contracted service providers, including our parent company, in:

(a) the UK, or

(b) the EU, where it has the same legal protection as in the UK, or

(c) by the parent company in the US, under an agreement approved by the Information Commissioner's Office as guaranteeing the same legal protection as in the UK (a "Standard Contractual Clauses" agreement).

If a service provider needs to store or process your Information in or access it from any other country, CPOMS will put in place measures approved by the Information Commissioner's Office that commit the service provider to the same level of data protection as is required under the UK Data Protection Act and UK GDPR.

Deletion

Information is deleted by termination of the agreement between the school and CPOMS. The school would need to formally contact CPOMS to express its wish to terminate the contract.

Will you be sharing the data with anyone?

Information is shared with secondary schools Year 6 children transition to once children are on roll and on the management of information system there. Information is also shared with schools children transition to and with safeguarding agencies and the police if necessary to keep the child safe.

There are different levels of access for staff, with the most sensitive data restricted to the trained safeguarding team, class teachers have access to most information for their class (apart from restricted safeguarding information), other staff can add information only.

What types of processing have been identified as 'high risk'?

We have screened the processing against a list of high-risk factors and identified that the main risks are:

- The personal data is highly personal in nature – concerns about safeguarding, SEND needs and behaviour are only shared with staff on a need-to-know basis and this kind of information could be damaging to a child's reputation and embarrassing if disclosed in error.
- The information concerns children – some of the children are particularly vulnerable because of home circumstances, having additional needs or other challenging circumstances of a personal nature.

Describe the scope of the processing:

What is the nature of the data, and does it include special category or criminal offence data?

How much data will you be collecting and using? How often?

How long will you keep it?

How many individuals are affected?

What geographical area does it cover?

Nature of the Data

The data relates to the behaviour and special needs of pupils – it will include special category data and would not usually include criminal offence data.

How much data will you be collecting?

We will be collecting and using data relating to pupil behaviour, special needs and safeguarding only, and not collect and share any more data than is required to achieve our purposes of tracking behaviour, meeting needs and fulfilling our safeguarding duty.

How often will you collect this data?

CPOMS will keep the data as long as the school's relationship continues with CPOMS and data is archived when a child leaves the school

How long will you keep it?

The school follows the good practice in terms of data retention as set out in the IRMS Information Management Toolkit for Schools. Information within CPOMS will be retained in line with the relevant retention schedules.

How many individuals are affected?
The data involves up to 420 pupils and 40 - 50 staff.

What geographical area does the processing cover?

Your Information may be stored and processed by CPOMS or by our contracted service providers, including our parent company, in:

(a) the UK, or

(b) the EU, where it has the same legal protection as in the UK, or

(c) by our parent company in the US, under an agreement approved by the Information Commissioner's Office as guaranteeing the same legal protection as in the UK (a "Standard Contractual Clauses" agreement).

If a service provider needs to store or process your Information in or access it from any other country, we will put in place measures approved by the Information Commissioner's Office that commit the service provider to the same level of data protection as is required under the UK Data Protection Act and UK GDPR.

Describe the context of the processing:

What is the nature of your relationship with the individuals? Do they include children or other vulnerable groups?

How much control will they have?

Would they expect you to use their data in this way?

Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in?

Are you following an approved code of conduct or certification scheme?

What is the nature of the relationship with the individuals? Does the processing involve children or other vulnerable groups?

The school are a data controller and CPOMS are the data processor. The data subjects are employees and pupils of the school.

The processing involves children who are automatically deemed to be a vulnerable data subject. It is school policy to inform all parents of the processing through our privacy notice.

How much control do individuals have?

Individuals and their parents do have the right to object. On receiving an objection, the school will consider the rights of the individual and balance these against the school's interests and inform the objector of the outcome. However, as this kind of processing falls within the school's public task, it is anticipated that individuals will not have significant control over the processing. The school will be transparent about the processing and only record information that is necessary and proportionate in achieving its aim.

Would they expect you to use their data in this way?

The children who will be monitored as part of the programme will be pupils that we have identified to be disengaged or who are exhibiting challenging behaviour, have additional needs or require safeguarding concerns to be recorded. Therefore, their parents will be aware that special focus will be placed on them by the school. All children are subject to our duty of care regarding safeguarding under KCSiE 2022

Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in?

This technology is not novel, it has been used widely across schools for some time now. We are not aware of any concerns relating to this kind of technology

Are you following any approved Codes of Conduct?

There are currently no approved Codes of Conduct for this particular kind of processing. However, the school will continue to review guidance from the ICO and adopt any relevant guidance as it becomes available.

Describe the purposes of the processing:

What do you want to achieve from this processing? What is the intended effect on individuals?

We seek to use the application to track behaviour of pupils that we have identified to be disengaged or who exhibit challenging behaviour. Our goal is to identify behavioural trends of these pupils and subsequently tailor our approach to improving their behaviour. We hope that over time this increases the efficiency of senior management staff and improves communications between the school and parents on the issue of behaviour.

The intended effect of individuals is to highlight trends of their behaviour to them, which we believe will make them more self-aware of their behaviour, and subsequently to help them improve their behaviour in school.

We seek to use the application to track safeguarding concerns and information in relation to our pupils that we have identified as raising a concern. Our goal is to identify safeguarding patterns and trends of these pupils and subsequently tailor our approach to keeping them safe. We hope that over time this increases the efficiency of senior management staff and improves communications between the school, parents and external agencies.

We seek to use the application to track SEN concerns and information in relation to our pupils that we have identified as raising a concern. Our goal is to identify patterns and trends of these pupils related to possible additional needs and conditions and subsequently tailor our approach to meeting their needs. We hope that over time this increases the efficiency of senior management staff and improves communications between the school, parents and external agencies.

What are the benefits of the processing – for you, and more broadly?

The benefits of processing will be increased efficiency amongst senior management staff, improved reporting from the school to parents regarding behaviour, SEN and safeguarding concerns/ information, and with external agencies as necessary.

Step 3: Consultation process

Consider how to consult with relevant stakeholders:

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so

We have not sought parents' views as this kind of data processing is not novel or unexpected. We are doing this electronically but do not believe it to pose any more risks than keeping paper records which schools are required to do.

Who else do you need to involve within your organisation?

Staff have received appropriate training on using the system and receive updates as needed.

Do you plan to consult information security experts, or any other experts?

We have consulted with our DPO.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

What is your lawful basis for processing?

Does the processing actually achieve your purpose? Is there another way to achieve the same outcome?

If appropriate, how will you prevent the use of the technology or system beyond the purpose for which it was originally intended?

How will you ensure data quality and data minimisation?

What information will you give individuals?

How will you help to support their rights?

What measures do you take to ensure processors comply?

How do you safeguard any international transfers?

What is your lawful basis for processing?

Our lawful basis for processing is *public task*. The processing will enable us to achieve our goal of monitoring and improving pupil behaviour, safeguarding and SEN responsibilities at school.

Does the processing achieve your purpose and is there any alternative way to achieve the same outcome?

The processing will enable us to achieve the desired outcomes, as set out above. The alternative would be to keep paper records and assimilate information manually. However, this is inefficient, and poses its own risks (possibility of accidental disclosure, loss, or damage).

How will you prevent the use of technology or system beyond the purpose for which it was intended?

We have obtained assurances in writing from CPOMS that the data of pupils will only be used for the purposes of tracking behaviour and producing reports for the school. CPOMS will not use the data for any other purpose.

We have obtained a data processing agreement/contract/terms and conditions which is compliant with Article 28 of the UK GDPR. It ensures that CPOMS complies with its obligations.

Staff are provided with training on how to use this system to ensure that they only use the information in line with our specified purposes.

How will you ensure data quality and minimisation?

Only information that is necessary is recorded on the system. Any errors can be rectified immediately.

What information will you give individuals?

Individuals are made aware of the processing by way of our privacy notice which is published on the school's website.

What measures do you take to ensure processors comply?
The school have taken steps to ensure there is a written agreement in place with CPOMS containing the relevant clauses as defined under Article 28 of the UK GDPR.
https://www.cpoms.co.uk/privacy/

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
1. Retention of behavioural data for longer than necessary Risk to individuals – pupils' behavioral data may be retained by St Nicholas C of E Primary School for longer than is necessary Compliance risk – non-compliance with storage limitation principle Corporate risk – Loss of reputation	[Possible]	[Minimal]	[Low]
2. System or accounts hacked or accessed unlawfully, and information being used inappropriately. Risk to individuals: Possible identity fraud, embarrassment for pupils and families, possible risk of physical harm to pupils in extreme circumstances. Compliance risk: Non-compliance with security principle.	[Possible]	[Significant]	[Medium]

Corporate risk: Loss of reputation, fines and sanctions.			
3. Information used outside of the purposes for which it is intended. Risk to individuals: loss of control over data, data used for purposes of which the individual is unaware. Compliance risk: Non-compliance with purpose limitation principle and lawfulness, fairness and transparency principle, data used without lawful basis. Corporate risk: Loss of reputation, fines and sanctions.	[Remote]	[Significant]	[Low]

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/No
1. Retention of behavioural data for longer than necessary	The school's retention policy outlines the procedure to be undertaken on an annual basis to ensure data is not retained for longer than is necessary. We have obtained written assurances from CPOMS in the data processing agreement, that CPOMS can only retain data as long as it has a relationship with the school. It must delete data if the school terminates its agreement with CPOMS, or a pupil has left the school for more than a year	[Reduced]	[Low]	[Yes]
2. System or accounts hacked or accessed unlawfully, and information being used inappropriately.	Security through WCC systems and school is compliant with WCC requirements and measures	[Reduced]	[Medium]	[Yes]
3. Information used outside of the purposes for which it is intended.	The school will carry out audits to track system usage. There is a breach reporting procedure in place and only the information necessary will collected and processed.	[Reduced]	[Low]	[Yes]

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Sarah Rayson Dec 2023	
Residual risks approved by:	Governors Jan 2023	
DPO advice provided:	Dec 2022/ Jan 2023 Eniola Adebayo- Oyetoro	
Summary of DPO advice:		
DPO advice accepted by	Sarah Rayson	
Comments:		
Consultation responses reviewed by:		
Comments:		
This DPIA will be kept under review by:	School and DPO	