

Data Protection Impact Assessment (DPIA) St Marys

DPIA in relation to:
Provision of online education/ implementation of online learning platforms. The Microsoft Teams learning platform used during national lockdowns.
Name and Position of Individual(s) responsible for DPIA:
Laura Concannon Head Teacher Mrs Louise King Data Controller.
Assessment date:
September 2021
Review date:
December 2021

Step 1: Identify the need for a DPIA

SIMS pulls through class data- Childs full name/Email Address provided by the platform and class assigned to.
<p><u>The aim of using [The Learning Platform]</u></p> <p>We are using an online learning platform to enable us to meet our responsibilities of providing high quality education, remotely. We also use the online learning platform to enhance the learning of individual pupils of the school.</p> <p>The online learning platforms we are looking to engage include:</p>

- Microsoft Teams

Video communications:

- Pupils will log on to the platform and engage in video communications to replicate the classroom experience as much as possible. This will assist with pupil engagement. This will involve processing data relating to images and audio.
- Parents/individuals will be sent instructions on how to use the system and be informed on how to turn off the camera function and mute the microphone/the school will ensure all children will have the cameras and microphones switched off until invited to unmute their microphones when appropriate.
- Names of pupils will be visible to others (all students will already be familiar with individual names from their class).
- Children will/will not be able to use the chat function. This will be monitored to give reassurance to parents. The chat function will be disabled when the lesson has finished.

Recording sessions:

- Keeping in touch sessions will be recorded and retained in line with the school's retention policy (3 months). For the duration of retention, recordings will be kept on the school's secure server and only accessible to senior members of staff. The recordings will only be used if a safeguarding concern is raised. At the end of the recording retention period, they will be permanently deleted.

The benefits of using [The Learning Platform]

These online services promote the education of the pupils and allow us to deliver a good quality education when children are unable to attend school.

Why do we need to do a DPIA? Does this type of processing automatically require a DPIA?

A DPIA is to be conducted as we are sharing vulnerable subjects' data with an online processor. Where cameras are used, the processing has the potential to be more invasive as it allows others to see into the child's home and possibly other members of their family.

Step 2: Describe the processing

Describe the nature of the processing:

Videos of keeping in touch sessions will be kept for three months and then destroyed. They are only available to staff and are reviewed by the head teacher.

Collection

The following data will be processed.

- Video of keeping in touch sessions.
- Microphone and chat function controlled by class teacher.
- Videos stored in a secure location on the Shared Drive

Usage

The processor's contract/agreement has been consulted for this DPIA in terms of their security processes. The processor uses a password login to keep accounts secure.

Storage

The data is retained by the school for checking by the senior staff and will be stored on the learning platform for three months. The information received by teams are stored on servers in Cardiff and London.

Deletion

Recordings will be kept on the school's secure server and permanently deleted after 3 months.

Recordings may be shared with official organisations if a required as a result of a safeguarding concern. This will be in line with the School's safeguarding policy.

Will you be sharing the data with anyone?

Data is shared with the head teacher on the shared drive.

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

The criteria for high risk is that vulnerable subjects' data is being processed and shared with a processor. Children are less aware of the risks to their rights and privacy.

This includes images and audio, video communications and recordings of lessons. There is the potential for the processing to be more invasive because children and staff may be recording with their own homes, possibly with other family members around.

There is also the possibility that comments or images that captured could be personal in nature and cause embarrassment.

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 nature of the data is educational and personal identifiers.

How much data will you be collecting?

Pupil

Names

Images

Audio

Email address

Staff

Names

Images

Audio

Email address

How often will you collect this data?

Weekly keeping in touch sessions.

How long will you keep it?

The data will be processed in line with the school's retention policy. The data will be processed for these purposes for the duration of the lockdown.

How many individuals are affected?

The data involves 73 pupils and 5 staff.

What geographical area does the processing cover?

Data is stored within the EEA on a UK based server in London and Cardiff.

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?

Individuals are pupils at the school and would be considered vulnerable data subjects. The school owes a duty of care to our pupils so children's safety and best interests will be considered at all times.

How much control do individuals have?

If the data is processed on the grounds of consent, the individuals (or parents on their behalf) can withdraw consent at any time.

Where data is processed on the ground of public task, pupils (or parents/carers on their behalf) can object to the processing of their information in this way. The school will weigh up the interests of the pupils in accordance with their interests, rights and freedoms against the legitimate grounds for processing the data.

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

Individuals are likely to expect the use of their data in this way, as the expectation is that education will continue during periods of self-isolation or in the event of a local/national lockdown/individuals will expect their data to be used in this way for the purposes of providing their child with learning resources to assist with their education. Individuals will be informed via the privacy notice.

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?

Processing using a learning platform is not a novel processing activity and the majority of online learning platforms are well-established.

Currently, the school has limited online learning resources. Using this data processor will enable the school to fulfil their duty in providing high quality education remotely/assisting learners with their learning.

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? What is the intended effect on individuals?

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

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

The overall purpose is to ensure children can still have access to an education in the event of a local or national lockdown and/or during periods of self-isolation/the overall purpose is to enhance the learning of pupils attending the school and actively engage with their education

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

The benefits of processing are that pupils can work remotely, individually, using technology and results are recorded easily, allowing the teachers to process assessment/attainment data efficiently.

Targets can be set using online platforms and overall, this is in a timely manner in which to record the progress of pupils.

Children can continue with their learning from home, this will limit any disruption to their education in the event of self-isolation or closure of the school.

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.

Who else do you need to involve within your organisation?

Do you need to ask your processors to assist?

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

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

Seeking the views of individuals may not be appropriate in this scenario as this is a standard process of the school/is part of the school's contingency plan to ensure high quality education during periods of self-isolation or a national/local lockdown / The views of the individual will be taken into account when seeking consent.

Who else do you need to involve within your organisation?

We have also consulted with staff at staff meetings over the past few weeks and have ensure that they have received appropriate training on using the system.

We have involved our Capita team who are employed by the school to manage the platform.

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

We will seek advice from our Data Protection Officer via this Data Protection Impact Assessment/we will consult our IT support.

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?

Where the processor is not a routinely used system, consent will be gained, and *consent* will be our lawful basis.

Where this is the schools adopted method of teaching/educating, the lawful basis will be *public task* (essential for running the school). The processing helps to achieve the purpose of educating pupils.

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

Alternative measures, such as paper assessments or quizzes can be used, but the online platform offers a simple, quick and effective tool for learning. /The school is required to provide high quality education during periods of self-isolation or in the event local/national lockdown.

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

Controls can be used to disable the use of the platform for any users. Activity is monitored.

How will you ensure data quality and minimisation?

Only the personal data necessary for the performance of the online platform, as set out in the GDPR compliant contract, will be collected for processing. Any incorrect information will be amended, although it is not anticipated that any accidental errors could have a significant impact on individuals if they were to occur.

What information will you give individuals?

Parents and pupils will be notified via the privacy notice on the school's website OR parents/pupils will be notified via the summary notice on the consent form.

How will you support individual's rights?

We will uphold the rights of individuals as set out below:

- **Right to be informed:** will be supported with the aforementioned notices and parents can visit the processor's privacy notice for more information.
- **Right of access:** this will be supported by the school's subject access request template on the website. The processor contract outlines that they will help the controller to achieve compliance with data protection obligations, which will include supporting the right to access.
- **Right to erasure:** will be supported where EITHER consent is removed OR a valid objection to the processing is received. The right to object is outlined in step 2.
- **Right to object:** individuals can exercise their right to object by contacting the school. If your lawful basis is consent We will consider each request on a case-by-case basis and determine whether the individual's right overrides or interest in processing the data to fulfil our public task. Reminders of this are also issued annually and details of how to exercise these rights are detailed within the privacy notice.
- **Right to restrict processing:** the right to restrict will apply where possible.
- **Right to data portability:** this may be requested in the event a child moves on to a different school where a similar system is used. The school will explore all options available to them in the event such a request was to be received.
- **Right to rectification:** the school will consider any other data that may need to be rectified and communicate this with the processor where this is deemed necessary. This is supported in the school's annual data collection/data checking sheets. However, specifically, pupils and their parents can update details at any point via the school's contact details. The processor allows for changes to login details when required.
- **Automated data processing:** there is no automated processing regarding the data.
- **Considerations to human rights:** the right to privacy may be impacted due to video communications resulting in teachers and other individuals hearing and seeing what goes on in people's homes. To mitigate this risk, individuals will have the option to/teachers will ensure cameras and microphones are switched off.

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 Remote, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high
<p>1. Hacking into processor site</p> <p><u>Risk to individuals</u> – access to video recordings/learning information [adapt as necessary]</p> <p><u>Compliance risk</u> – non-compliance with security principle</p> <p><u>Corporate risk</u> – Loss of reputation</p>	Remote, possible or probable	Minimal, significant or severe	Low, medium or high [Low]
<p>2. Loss of login passwords/username and or loss of access into the site</p> <p><u>Risk to individuals</u>: exclusion from learning</p> <p><u>Compliance risk</u>: Non-compliance with security principle.</p> <p><u>Corporate risk</u>: Loss of reputation</p>			[Low] This can be reset easily.
<p>3. Data used outside the scope of its original purposes</p> <p><u>Risk to individuals</u>: loss of control over data, data used for purposes of which the individual is unaware.</p> <p><u>Compliance risk</u>: Non-compliance with purpose limitation principle and lawfulness, fairness and transparency principle, data used without lawful basis.</p> <p><u>Corporate risk</u>: Loss of reputation, fines and sanctions.</p>			[Medium]
4. Impacts on individual's right to privacy			

<p><u>Risk to individuals</u>: loss of control over data, images disclosed that should not have been, invasion into private life.</p> <p><u>Compliance risk</u>: Non-compliance with lawfulness, fairness and transparency principle.</p> <p><u>Corporate risk</u>: Loss of reputation, fines and sanctions.</p>			[Medium]
--	--	--	----------

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?
1. Hacking into processor site	Capita and schools broadband monitor the security.	Eliminated reduced accepted [Reduced]	Low medium high	Yes/No
2. Loss of login passwords/username and or loss of access into the site	Issued and set by head teacher.		[Low]	
3. Data used outside the scope of its original purposes	The contract/agreement meets the requirements of GDPR – assurances are given in the legally binding contract for the purposes for which the data will be used/processed. School staff are briefed and aware of the school's data protection and information security policy.	[Reduced]	[Low]	[Yes]

4. Impact on rights to privacy	<p>For children using the function as a form of social media, rules on using the system will be in place and this will be monitored/chat functions will be disabled at all times/at the end of each lesson.</p> <p>Individuals will have the option to turn off their camera and mute their microphone/teachers will ensure all participants mute their microphone and turn off the camera function. Pupils will be invited to unmute their microphone when appropriate for engaging in the lessons and then asked to unmute again. Parents will be made aware of the lessons and timetables and given the opportunity to voice their concerns and exercise their right to object.</p>	[Reduced]	[Low]	[Yes/No]
---------------------------------------	--	-----------	-------	----------

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Laura Concannon	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	DPO Warwickshire service (see email print out)	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	The School DPO Service (Warwickshire Legal Services) 15/12/2021	DPO should advise on compliance, step 6 measures and whether processing can proceed

<p>Summary of DPO advice:</p> <p>The DPIA considers all of the relevant risks to individuals and mitigating measures have been put into place. Any residual risk is low. We are satisfied that the project has been thoroughly considered and the processing can proceed in compliance with data protection legislation.</p>		
DPO advice accepted or overruled by:	Accepted 15/12/21	If overruled, you must explain your reasons
<p>Comments:</p>		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
<p>Comments:</p>		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA