DPIA

This DPIA follows the process set out in the ICO DPIA guidance.

Submitting controller details

|  |  |
| --- | --- |
| Name of controller | Nautilus Education |
| Subject/title of DPO | Nautilus |
| Name of controller contact /DPO | David Rushby |

Step 1: Identify the need for a DPIA

|  |
| --- |
| Explain broadly what 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. |
| The Nautilus School Leadership Platform is designed to offer comprehensive data analytics insights focused on teaching and learning. It also gathers anonymous feedback from pupils and parents. The system compiles this information into summaries and charts, enabling school leaders to identify both strengths and areas needing improvement.  Additionally, photos can be utilised to assess pupil learning, the impact of the curriculum, and the quality of student work.  Given the innovative approach and objectives of the solution, we determined that conducting a Data Protection Impact Assessment (DPIA) was necessary. |

Step 2: Describe the processing

|  |
| --- |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
| Data, staff feedback and photos are collected via tablets and computer on site in school. Occasionally, staff may work from home also to prepare or utilise the system.  All data is stored at Amazon Web Servers London. Cloud security at AWS is the highest priority. AWS customers benefit from data centres and network architectures that are built to meet the requirements of the most security-sensitive organisations. Use the following documentation to [learn more](https://docs.aws.amazon.com/security/) about your security and compliance objectives. Any data deleted is by the end user or when the company closes the subscription.  No data is shared by the company. All data is for internal use and controlled by the school (end user).  The school accesses and administrates a cloud-based platform.  The school adds the staff to the system using name and work email. No other personal data is within the system.  Leaders then evaluate teaching and learning using a series of frameworks. Any external leaders such as school improvement partners or professional partners can be added to the system with restricted access.  Feedback, analysis and reports is presented and accessed by the school internally.  There are no requirements for pupil data.  Any photos of pupils within the system are captured with the discretion of the school policy. All photos are secure, stored internally and used for professional purposes. For best practice, align or integrate this expectation within the school presentation and/or data management policy.  Where the school chooses to upload or record photographs or videos of pupils or staff, such media is treated as personal data under the Data Protection Legislation. These images are used to support professional development, curriculum evaluation, and school improvement. All media is stored securely, used only for internal professional purposes, and retained in line with the school’s instructions. No biometric or facial recognition technologies are used.  The platform may also use artificial intelligence (AI) technologies, including services provided by OpenAI, to support the analysis of lesson observation data. This processing enables the identification of pedagogical patterns, enhances reporting functionality, and informs leadership and professional development strategies. Where personal data is involved, AI processing is conducted under documented instruction from the school and in accordance with applicable data protection legislation. Outputs are used solely for educational improvement purposes and are subject to appropriate safeguards. |

|  |
| --- |
| **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? |
| The data collected includes:  The date of the observation  The staff involved  The area of study or lines of enquiry  The name of the school  The data is collected across the school year as per the school monitoring calendar.  The data will remain live for the duration of the subscription. When the subscription closes, all data is deleted.  When leaving the school, the school administrator can delete the related teacher insights. |

|  |
| --- |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? 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 signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| The individuals withing the system will be employees of the school or associated partners. This system enables all school leaders to be able to manage workload, secure school improvement and gain strategic insights to support their roles and responsibilities.  The data collected would also be used for professional development and appraisal purposes. This is typical within schools to support pay and career progression.  No concerns about the data procession have been raised. The company intentionally uses a minimal amount of data to maximise the impact of the system.  The company is registered with the ICO.  The company provides a Privacy Notice.  The company provides evidence of professional indemnity insurance |

|  |
| --- |
| **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? |
| The data is used to quality assure and self-evaluate the schools provision. This is an internal process that enables the school leaders to identify strengths and areas for development.  The data is used to help individual teachers to collaborate and to facilitate professional development. This is in the form of analysis and feedback, with reports to support continued professional development.  The system does not provide anything that would be exceptional. These are standard procedures within school that are part of the effective day to day running of the school.  The benefits of the system relate to professional development and improved outcomes for children. The data directly enables the school staff team to improve teaching and learning. |

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? |
| All of the hosted individuals would be expected to engage in a process of individual and school improvement. This is not optional as documented in the expected national standards. The system enables schools to manage this more efficiently and collaboratively. How the school chooses to do this is independent to the themselves. Using software to aid this process is entirely typical, as well as documentation and evidence stored electronically.  Consultation with regards to best practice with the staff team would be recommended. This could include the frameworks and language used, how to support underperformance and how to reward contributions.  The system enables the school to improve outcomes for pupils, secure school improvement, and support professional development. The company does not take responsibility for how the data and feedback is presented or used within the school to address individual or whole school performance, competency or behaviour.  Schools are encouraged to consult staff on the use of photographic and video data, including how it supports professional development and curriculum evaluation. This should align with the school’s data protection and safeguarding policies. The company provides guidance on secure use and retention, but does not control how media is interpreted or presented within the school. |

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? How will you prevent function creep? 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? |
| We are using the data to provide opportunities for the school to identify whole school and individual teacher strengths and areas for development. We endeavour to ensure that the required data is minimal, with limited insights required to effectively support school improvement.  By using AWS, we are actively ensuring that the data management security is as effective as possible. This storage option is constantly updated, review and tested to ensure maximum protection. |

|  |  |  |  |
| --- | --- | --- | --- |
| Step 5: Identify and assess risks | | | |
| **Describe source of** risk **and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm**  Remote, possible or probable | **Severity of harm**  Minimal, significant or severe | **Overall risk**  Low, medium or high |
| **1a Unauthorised internal access to the platform**  Access to professional emails whole school statistical analysis and teaching evaluations. | x |  |  |
| **1b Unauthorised external access to the platform**  Access to professional emails whole school statistical analysis and teaching evaluations. | x |  |  |
| **1c External partner access**  Access to professional emails whole school statistical analysis and teaching evaluations. | x |  |  |
| **1d Sharing content, reports or information**  Potentially sensitive feedback or data | x |  |  |
| **1e Photo-sharing or exporting**  Misuse such as social media or sharing | x |  |  |
| **1f Lost passwords**  Unauthorised access | x |  |  |
| **1g Change of administrator**  Inability to manage the system | x |  |  |
| **1h Lost hardware with shortcuts or cookies** | x |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | | **Likelihood of harm**  Remote, possible or probable | **Severity of harm**  Minimal, significant or severe | **Overall risk**  Low, medium or high |
| 1a Unauthorised internal access to the platform | Ensure that individual passwords are safely stored. Make sure password are sufficiently secure. Don’t’ use autofill.  Try not to use the same devices as the pupils.  Always log out. | Possible | Minimal | Low |
| 1b Unauthorised external access to the platform | Ensure that individual passwords are safely stored. Make sure password are sufficiently secure. Don’t’ use autofill.  Try not to use the same devices as the pupils.  Always log out. | Remote | Minimal | Low |
| 1c External partner access | Only add verified users.  DBS checked. | Probable | Minimal | Low |
| 1d Sharing content, reports or information | Discuss and publish protocols.  Only use professional emails.  Internal school use only. | Possible | Minimal | Low |
| 1e Photo-sharing or exporting | Publish protocols.  Professional use.  No names or personal info tags  No exporting or sharing | Possible | Minimal | Medium |
| 1f Lost passwords | Ensure secure password guidance  Store safely  Change periodically | Possible | Minimal | Low |
| 1g Change of administrator | Update the company | Possible | Minimal | Low |
| 1h Lost hardware with shortcuts or cookies | Ensure that devices do not autofill  Manage device access and security | Remote | Minimal | Low |

Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/position/date** | **Notes** |
| Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: |  | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: |  | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| DPO advice accepted or overruled by: |  | If overruled, you must explain your reasons |
|  |  |  |
| Comments: | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |