Data Protection Impact Assessment

PrimarySite

Date: 25/11/2024

Juniper

Contents

Data Protection Impact Assessment (DPIA)

How to complete a DPIA

A DPIA must be carried out if new technology is being deployed or there is a change to the nature, scope, context or purposes of existing processing activities which meets any of the criteria below.

There are guidance notes in Appendix A to assist you in completing the form.

Screening

The DPIA comes in two parts: the first part is a short screening questionnaire, which requires you to answer a set of questions to establish whether certain data processing operations, activities or processes will impact upon the rights and freedoms of data subjects.

Full DPIA Assessment

Where you have answered yes to one or more of the screening questions in Part 1, you must complete Part 2 to document the assessment of the impact of the processing activities.

Part 1

DPIA Screening

Describe the project/processing/system etc. and, if it is new or a variation to existing, explain why it is being introduced. Include the objectives of the processing.

The Primarysite CMS is used by schools to add content that parents, ofsted and the wider community can consume. The CMS will require staff log in credentials as well as parent and pupil data for the purposes of text messaging, emails, app verification, app messages and parents evening bookings.

The CMS also powers a mobile application where parents are invited and verified to receive content from school via the app.

There are 2 objectives to processing the data:

1. To enable staff to log in with their school email address.
2. To view and segment parent and pupil data to communicate with parents.

DPIA Screening Questions

Complete this section to help determine whether the processing is likely to result in a risk to the rights and freedoms of data subjects. Use the guidance in Appendix A to assist you. Where the answer is yes/true, indicate this in the relevant checkbox.

You should **consider** carrying out a DPIA if you plan to carry out any of the following:

☐ This a major project involving the use of personal data;
☐ Evaluation or scoring;
☐ Systematic monitoring;
☒ Processing sensitive data or data of a highly personal nature;
☒ Large scale processing activities;

You **must always** carry out a DPIA if you plan to:

☐ Process special-category data or criminal-offence data on a large scale;-
☐ Process personal data that could result in a risk of physical harm in the event of a security breach;
☒ Process personal data concerning vulnerable data subjects;
☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or to offer online services directly to them;
☒ Process biometric or genetic data;
☐ Systematically monitor a publicly accessible place on a large scale;
☐ Process personal data without providing a privacy notice directly to those affected;
☒ Process personal data in a way that involves tracking individuals' online or offline location or behaviour;
☐ Use systematic and extensive profiling or automated decision-making or special category data to make significant decisions about people including decisions on someone's access to a service, opportunity or benefit;
☐ Combine, compare or match data from multiple sources;
☐ Use innovative technology or technology in innovate ways;
☐ Processing that involves preventing data subjects from exercising a right or using a service or contract.

If **any** of the boxes above are ticked, a DPIA **must** be carried out. Complete and sign below then complete Part 2 of this form.

If none of the boxes above are ticked a DPIA is not required. Complete and sign below then forward this form to the DPO@junipereducation.org

Date of DPIA Screening	25/11/2024
Result of DPIA Screening	Full DPIA required

*Delete one option

Part 2

About the Processing

What data is being processed?

Tick all that apply

☒ Name
☒ Other identifiers e.g. ID, username, etc.
☐ Financial information
☐ Religious Beliefs, Trades Union Membership or Political Opinions
☐ Medical/Health information or information about disabilities
☐ Criminal offences/convictions
☐ Information about behaviour–
☒ Audio or video recordings (e.g. CCTV images) or photographs
☒ Location data
☒ Biometric or genetic information
☐ Profiling
☒ Other (please state below):

Email address, mobile number

Who is the data about?

Tick all that apply

☒ Employees, former employees, or prospective employees incl. volunteers etc.
☒ Customers, former customers, or prospective customers
☐ Suppliers, former suppliers or prospective suppliers
☒ Members of the public

Describe the people whose data is being processed below. Include a description of the nature of the organisation's relationship with data subjects and whether the processing might include children or other vulnerable groups.

School staff members and governors – Username and password, photos and videos. Parents – name, email address and mobile number. Schools may also set parents up as "parent" users in the CMS. In this instance parents would also have their username and password processed. Children – Name, year group, class, photos and videos. Juniper staff within the website product, sales, support, engineering, finance, growth– accessing the PS back office to access all customer sites.

Would the people whose data is being processed expect their personal data to be used in the ways envisaged? Include a justification if it is within their reasonable expectations.

Yes, staff members will be invited to the CMS as a user if required by the school. Parents will also expect for their (and their childrens) details to be used by the school to communicate with them.

Purpose of the processing

What are the aims of the processing? What does the organisation want to achieve from it? If the data is pre-existing, how will the new use/processing differ from the current use/processing?

Staff – to be able to access the CMS and edit content. The school may also wish to communicate via the CMS with their staff.
Governors – to have access to read only areas.
Parents – to communicate with the parents.
Children – to segment the communication by childrens data (year group, class), photos on the front end of the website.

Website admin
School staff, governors and parents
Names and email addresses are used for the purpose of logging into a schools website. The schools will control who has access to their schools website CMS.

Contact Forms
Parents and/or members of the public
The CMS has the option of data capture which can be turned on by the school to gather enquiries.

MIS integration
Parents and children data
In order to operate efficiently, PrimarySite has to collect and use information from a school MIS (Management Information System). These may include current, pupils and parent contacts. MIS integration is required for text, email, parents evening and app notifications.

Manually added contacts
Parents and children data
If the school does not have MIS integration, they can add contacts to the CMS which is used to contact parents/carers by text or email.

Responsibility/Beneficiaries

Who in our organisation is taking responsibility for the processing? Who stands to benefit from the processing and how? What are the intended effects on individuals? How will they benefit?

Provision of the CMS – Engineering
Onboarding – Service Delivery
Ongoing support and off boarding – Support
Contracts and invoices – Sales and Finance
Product management – Product
Account management – Growth

Benefit commercially and inform the future of product development.

Nature and context of the processing

Describe the processing activities and their purpose. Provide sufficient context to enable the reader to understand how and why the processing occurs. Include information about how data will be collected, used and stored; the scale size and frequency of processing as well as who will use the information and for what purpose(s). If the processing is novel in any way, please describe how.

Website admin and manually added contacts are processed via the CMS technology and is either stored within the CMS and server/s.

The contact form data is not stored within the CMS. This data is outputted via email to the school's chosen email address.

MIS integration processing - PrimarySite processes data through a secure API integration with Wonde.

Email address for user management – to access the CMS
Email address for communications – to receive communications from the school
Mobile number – to receive communications from the school
Biometrics – to password protect TheSchoolApp

Parent and child data is processed using wonde as the integrator between the schools MIS and the CMS. Wonde updates twice daily.

IT Systems

What IT systems including hardware and software will be used for the processing?
Include data flows where possible that explain and visualise the processing activities and flow of data.

MIS data > Wonde > CMS
School create CSV and upload manually to CMS

Hardware:
Virtual Machines in Google Cloud Provider,
AWS holds static files and encrypted backups

Software:
Python + FreeBSD Jails

Disclosure and Sharing

Will the data be shared with any other people/organisations such as government agencies, data processors or sub-processors e.g. third party suppliers, application/website hosting companies, etc? ☒Yes ☐No
If yes, please list them below and include the purposes of the processing, their country and a link to their privacy notice.

Name	Purpose of processing	Country	Privacy Notice Link
Wonde	Sync data from MIS to CMS	UK	https://www.wonde.com/privacy-policy/
Google	To host the customer websites, also handles messaging	UK	https://cloud.google.com/terms/cloud-privacy-notice
AWS	To host media images and site data	UK	https://aws.amazon.com/privacy/
Matomo	To process webstats	UK	https://matomo.org/matomo-cloud-privacy-policy/
Twitter	Users can push website data like news, user controlled	US	https://x.com/en/privacy
Facebook	Users can push website data	US	https://www.facebook.com/privacy/policy/

	like news, user controlled		
Google / Mobile App	Firebase / to send push notifications Analytics / performance and usage patterns Crashlytics / Debug crashes and log bugs	UK	https://firebase.google.com/support/privacy https://support.google.com/analytics/answer/7318509?hl=en https://firebase.google.com/support/privacy

Consultation Process

The purpose of a consultation process is to understand the concerns and expectations of the individuals, test appropriate solutions and improve transparency.

Will the organisation be seeking the views of staff/customers/residents/other stakeholders regarding this processing? If not, why is this not necessary? If yes, describe the consultation process.

Product development – internal discovery and validation

Who else within the organisation will be consulted to ensure that all risks from the envisaged data processing are understood and properly mitigated?

Senior leadership team

Assessing the processing's necessity and proportionality

Are there alternative solutions which meet the goals without creating the same data processing risks? For example, a high-risk data processing activity which carries minimal benefit for individuals or significantly affects their data protection rights may not be proportionate. Further, if there is a feasible alternative which is of lower risk (e.g. one that makes less use of personal data), such activity may also not be necessary.

☐Yes ☒No

If there are no alternative solutions, consider whether the data processing complies with the data protection principles.

Rights

Where Juniper is the Data Controller, they are responsible for all data subjects' rights request. Where Juniper is processing customer data e.g. to provide software or services, they are the Data Processor.

Who is responsible for responding to data subjects' rights requests?

In relation to school data within PrimarySite, the customer is responsible for data subject requests.

Privacy Information

Does the Juniper Privacy notice provide sufficient information about how the data will be obtained and processed? If not, please contact DPO@junipereducation.org to have it added.
☒Yes ☐No

Lawful Basis

What is the lawful basis for processing the data? Tick all that apply

☐ Consent	☐ Vital interests	☐ Task by a public authority
☒ Performance of a contract	☐ Legal obligation	☒ Legitimate Interests

Is special category data processed? Special category data reveals racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); health; sex life; and sexual orientation.
☒Yes ☐No

If yes, what is the lawful basis for processing the special category data?

☒ Explicit consent	☐ Social security/protection law	☐ Legal defence or claim
☐ Employment law	☐ Vital interests	☐ Substantial public interest
☐ Public health interests	☐ Preventative/occupational medicine	☐ Archiving in public interest
☐ Data manifestly made public by data subject	☐ Scientific/historical research or statistical purposes	

Purpose Limitation and Minimisation

What measures have been taken to ensure that any personal data collected or created in this processing is not used for any purpose other than that documented in this DPIA?

Wonde integration with the MIS ensures that only data needed for parental communications is requested.

For user management, the user name is auto generated from the first and last name.

Images and content in the CMS cannot be copied or saved by the end user.

What measures have been taken to ensure that only adequate and relevant information is used in the processing and that it is limited to only that which is necessary to achieve the processing aims?

Through the wonde integration we only bring in the data that is relevant to the purpose of communicating with parents.

Accuracy

What measures have been taken to ensure that personal data is accurate? Is there a requirement to keep any personal data up-to-date? Could there be any negative consequences if the personal data is not kept up-to-date?

For parent data the data is managed in the MIS or manually uploaded into the CMS. Once the data is loaded, it cannot be amended. Any changes would require a re-sync or re-upload.

For user management – only super users can amend user credentials (excluding passwords)

Storage Limitation (Retention)

What is the retention period for the various types of personal data? If you cannot specify a specific retention period, what are the criteria that determine if the information is no longer needed, e.g. fulfilment of contract? How will the information be treated, e.g. returned/destroyed when it reaches the end of its retention period?

The website data base is stored with Google, London.
Content data is stored with AWS, Ireland.

PrimarySite will process personal data for the duration of the contract. Back-ups of website data will be stored for 6months. The destruction process is automated using AWS S3 Storage Account Lifecycle for deletion.

Security

Describe the security measures that will be implemented to ensure the confidentiality, integrity, availability and restorability of the data, data systems and processes?

Physical access to the servers is restricted by personal ssh-key and VPN requirements. Backups are encrypted and scripts present for restoration of data where required. Software systems are redundant over multiple availability zones within the GCP eu-west data centre load balanced. Sites are connected to via SSL generated through automated lets-encrypt processes for public access. School access uses our secure site for modification which is also SSL RSA-SHA256 encryption. Disks associated with the servers are secure for data at rest using GCP disk encryption which uses AES-256 encryption more details can be found here https://cloud.google.com/docs/security/encryption/default-encryption.
User passwords are encrypted using the bcrypt algorithm.

Juniper

WE LOOK AFTER YOU, SO THAT YOU CAN LOOK AFTER OUR CHILDREN

Junipereducation.org