



Data Protection Impact Assessment



Juniper Events

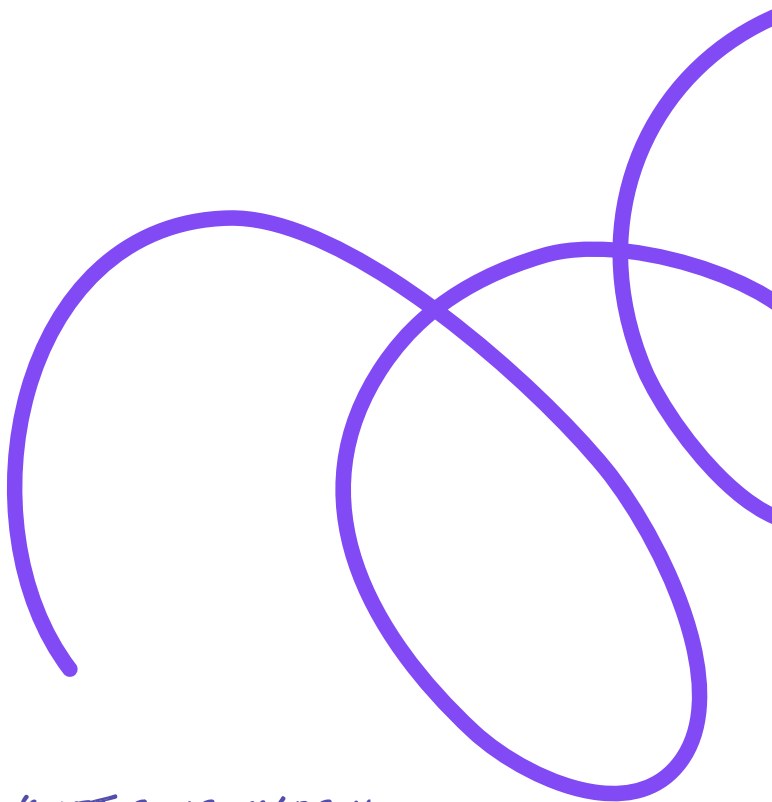
Date: 22/06/2026



Juniper

Contents

Data Protection Impact Assessment (DPIA)	3
How to complete a DPIA	3
Screening.....	3
Full DPIA Assessment	3
Part 1.....	3
DPIA Screening	3
Part 2.....	5
About the Processing.....	5



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 Events system enables schools to create, manage, and administer school events, including clubs, trips, and parents' evenings. Parents will also be able to book events and pay where required.

This is a new product offering, expanding on existing school data usage by introducing structured workflows for:

- Event creation and management
- Targeted invitations to parents to book enrichment for their children
- Parent booking and payment
- Staff allocation to events
- Reporting and administration of event participation and payments

Why it is being introduced: Schools currently rely on fragmented systems (e.g. spreadsheets, emails, paper forms, or multiple software tools) to manage events. This leads to:

- Increased administrative burden

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

- ~~Inefficiencies and duplication~~
 - Reduced parent engagement
 - Limited ability to target opportunities appropriately

This system is introduced to streamline event management, improve communication, and support schools in delivering enrichment opportunities more effectively.

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:

- A major project involving the use of personal data;
- Deploy new software/application/technology;
- 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	22/06/2026
Result of DPIA Screening	Full DPIA required

*Delete one option

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

Part 2

About the Processing

What data is being processed?

Tick all that apply

- Name and titles/job titles
- Other identifiers e.g. ID, username, etc.
- Personal address/postcode
- Business address/postcode
- Personal contact details, phone, email, etc.
- Business contact details, phone, email, etc.
- Bank details/financial information
- Employment details including salaries and benefits
- Absence data
- Performance data
- Next of kin
- Special Category data (race, religion, trade unions, health, disability, political opinion, sexual orientation, biometrics etc.)
- Criminal offences/convictions
- Information about behaviour
- Audio or video recordings (e.g. CCTV images) or photographs
- Location or ip data
- Other (please state below):

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.

The processing involves the following categories of data subjects:

Pupils:

- Primary data subjects
- May include **vulnerable groups**, including those with special educational needs (SEN) or those identified through characteristics such as Pupil Premium and Free School Meals.

Parents / Guardians:

- Linked to pupil records
- Receive communications, invitations, and booking functionality
- Act on behalf of pupils in booking and payment processes

School Staff:

- Teachers and administrative staff
- Assigned to events (e.g. running clubs, attending trips, hosting parents' evenings)

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, they also provide permission for access to their data to use the product.

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?

The aim is for customers to be able to create and manage events easily.

Schools act as data controllers for pupil, parent, and staff data

Through the provision of the system, Juniper operates as a data processor on behalf of the school. There is an established and expected relationship between:

- Schools and pupils
- Schools and parents
- Schools and staff

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?

The product processes personal data to enable the end-to-end management of school events, including creation, invitation, booking, payment, and reporting.

Data Collection:

Data is sourced from the schools MIS and may include:

- Pupil data (name, year group, characteristics)
- Parent/contact data (name, contact details, relationship to pupil)
- Staff data (name, role)
- No unnecessary or excessive data is collected.

How Data is Used:

- Event Creation & Targeting
 - Schools create events (clubs, trips, parents' evenings)
 - Pupils are selected based on:
 - Year group
 - Eligibility

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

▪ Characteristics (where relevant for inclusion or support)

- Invitations & Communication
 - Parents receive notifications via the app
 - Invitations are linked to their child/children
- Booking & Participation
 - Parents:
 - Book places
 - Complete forms (e.g. trip consent)
 - Select time slots (parents' evening)
- Payments
 - Payments are processed securely via Stripe
 - Transaction data is recorded and made available to schools
- Staff Allocation
 - Staff are assigned to events and schedules
- Reporting
 - Schools can:
 - View participation
 - Track payments
 - Export reports

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.

Data is collected via Portal and passed to the Events product.

The data between the schools MIS and portal synchronised daily. However there is a instant sync between portal and events. Content and data also syncs on refresh between events and the mobile app.

This data is used to create events and invite parents to book and pay.

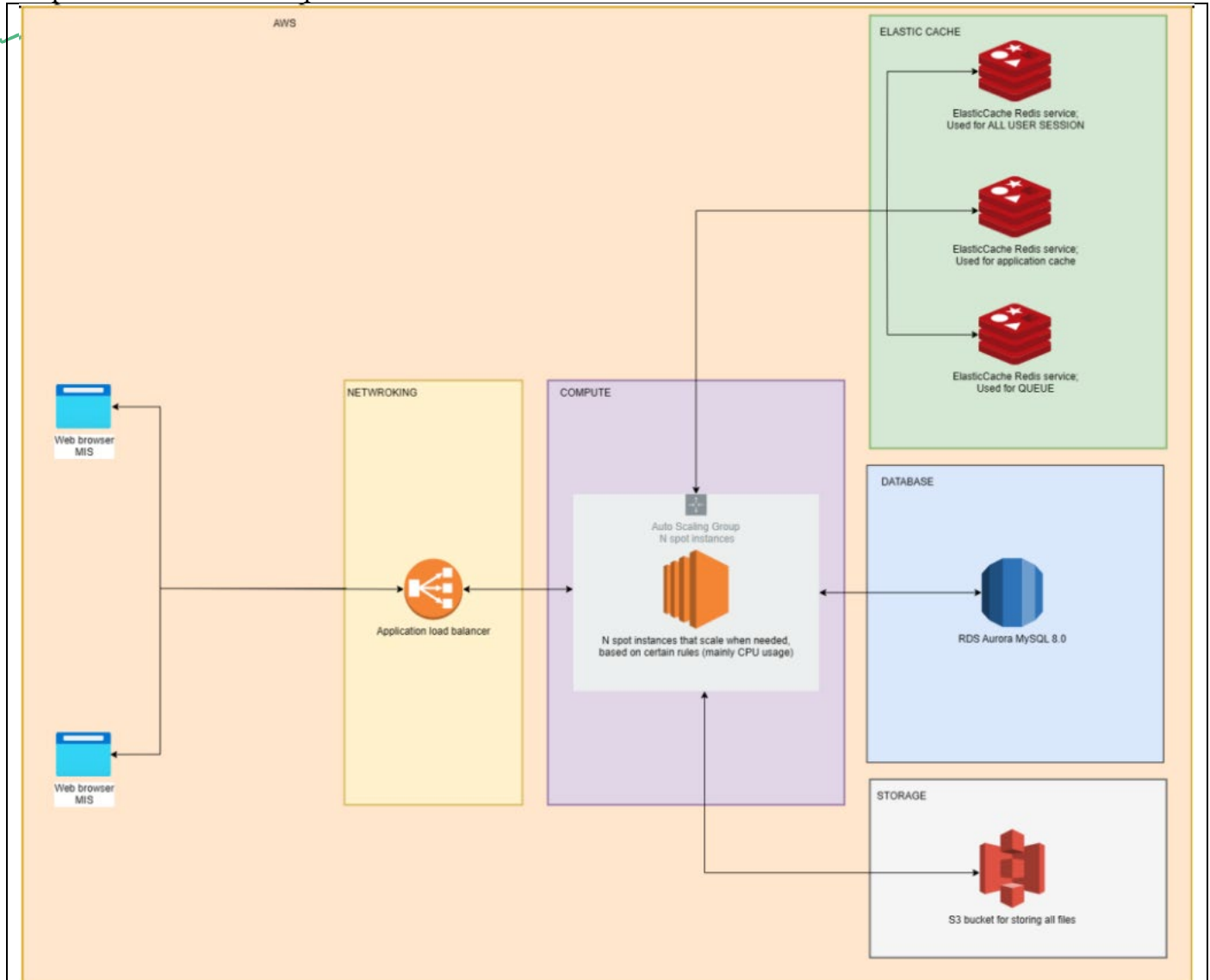
The Events products records the bookings and payments and provides appropriate reports to schools so they can track the events.

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.

Juniper Events is based on the AWS cloud computing stack. The structures and related products are outlined below.

Juniper Data Protection Impact Assessment



Events

The Events application is hosted within AWS and can be split into the following structures:

Networking - Amazon Elastic Load Balancing

Compute - Amazon EC2 Spot Instances

Cache - ElastiCache Redis (cache, sessions, asynchronous queues)

Database - RDS Aurora

Storage – S3

CloudWatch – stores application logs

ETL Tooling

The ETL tooling is hosted within AWS. It takes data from an input source and outputs it to Juniper MIS.

This process uses the following systems:

Database – MySQL

Web Server – Apache

Files - S3 / NFS

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

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

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
Stripe	Processing payments	UK	Privacy notice
AWS	Hosting	UK	Privacy Notice

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.

Yes, Juniper seeks the views of staff, customers, and other stakeholders during the discovery and validation phases of product development. The consultation process includes surveys, focus groups, interviews, and workshops to gather and analyse feedback, ensuring the product meets stakeholders' needs and expectations.

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

If a risk is identified as a concern under our legal obligation, this will be discussed immediately with Senior Leadership who will determine the best route in this project.

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?

Where Juniper is the processor, providing products and services under contract to a customer, the customer is the Data Controller responsible for rights' 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

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

Lawful Basis

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

<input checked="" type="checkbox"/> Consent	<input type="checkbox"/> Vital interests	<input type="checkbox"/> Task by a public authority
<input checked="" type="checkbox"/> Performance of a contract	<input type="checkbox"/> Legal obligation	<input type="checkbox"/> 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?

<input type="checkbox"/> Explicit consent	<input type="checkbox"/> Social security/protection law	<input type="checkbox"/> Legal defence or claim
<input type="checkbox"/> Employment law	<input type="checkbox"/> Vital interests	<input type="checkbox"/> Substantial public interest
<input type="checkbox"/> Public health interests	<input type="checkbox"/> Preventative/occupational medicine	<input type="checkbox"/> Archiving in public interest
<input type="checkbox"/> Data manifestly made public by data subject	<input type="checkbox"/> 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?

Juniper Education is committed to ensuring personal data collected is used only for the purposes documented in this DPIA and as outlined in our agreements with schools. Here are some key measures we have implemented:

- Access Controls: A robust, central user management system access control system provides access to school staff who require product access.
- Data Retention Policy: Outlined in Terms of Business.
- User Training: Juniper Education provides regular training to its staff on data protection principles and ensure they understand the importance of using personal data only for authorised purposes.
- User access to the platform is controlled through FusionAuth MFA and role-based access controls. Least-privilege principles ensure users only access data relevant to their functions. Administrative access is tightly restricted and monitored, and internal access management processes ensure appropriate approval, review and revocation cycles.

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?

The events product only uses data processed by Portal, which has also been authorised by the school.

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?

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

All data processed is centrally managed from a schools MIS. Therefore there is always one source of truth.

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 Events product will delete data in accordance with our standard data retention policies, with one exception.

In the case where a pupil leaves school, the data will continue to be processed and accessed in the product due to a specific need for evidencing participation and payment transaction reconciliation. In this case, the data will be retained in viewable in the product for 2 academic years after the pupil has left. After 2 academic years, the pupil will be anonymised

This ensures that schools are able to identify pupils that took part in events, allocate payments to them and perform any refunds if necessary.

Security

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

AWS hosting environment is secured using a default-deny approach. Firewalls and Security Groups block all traffic unless explicitly permitted. AWS native detection and prevention services (such as GuardDuty and baseline monitoring) provide additional protection. Configuration of network infrastructure is managed by a qualified third-party provider under least-privilege principles.

Logging of application behaviour, warnings, errors and user related changes is maintained within AWS CloudWatch. AWS alarms support detection of anomalous activity, service failures or performance issues, with further improvements planned.

Juniper adheres to secure coding practices governed by the organisation's Secure Development Policy. Source code is protected through controlled GitHub access, encryption of secrets/keys, and RBAC. All material changes follow a formal change-control process using Bitbucket and Jira, with hot-fix workflows for urgent corrective actions. Framework patching is carried out through a combination of automated and manual updates to ensure vulnerabilities are addressed promptly.

User access to the Events platform is controlled through FusionAuth MFA and role-based access controls. Least-privilege principles ensure users only access data relevant to their functions. Administrative access is tightly restricted and monitored, and internal access management processes ensure appropriate approval, review and revocation cycles.

All data is encrypted in transit and at rest within AWS. Automated point-in-time backups are maintained to allow restoration of data if needed. Backup processes follow AWS best-practice retention and integrity validation, with rapid PIT (Point-In-Time) restoration available to support continuity.

Automated AWS backups and PIT restoration procedures ensure data can be restored following an incident. These processes support Juniper's business continuity commitments and help ensure service availability and data restorability.

An external security provider performs regular vulnerability assessments across Juniper's network to identify risks and ensure continuous security hardening.



Juniper

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

[Junipereducation.org](https://www.junipereducation.org)

© 2023 Juniper Education Services Ltd. All rights reserved. This publication is the intellectual property of Juniper Education and no part of it may be reproduced, stored or transmitted by any means without prior permission of Juniper Education. Any unauthorised use for commercial gain will constitute an infringement of copyright.

