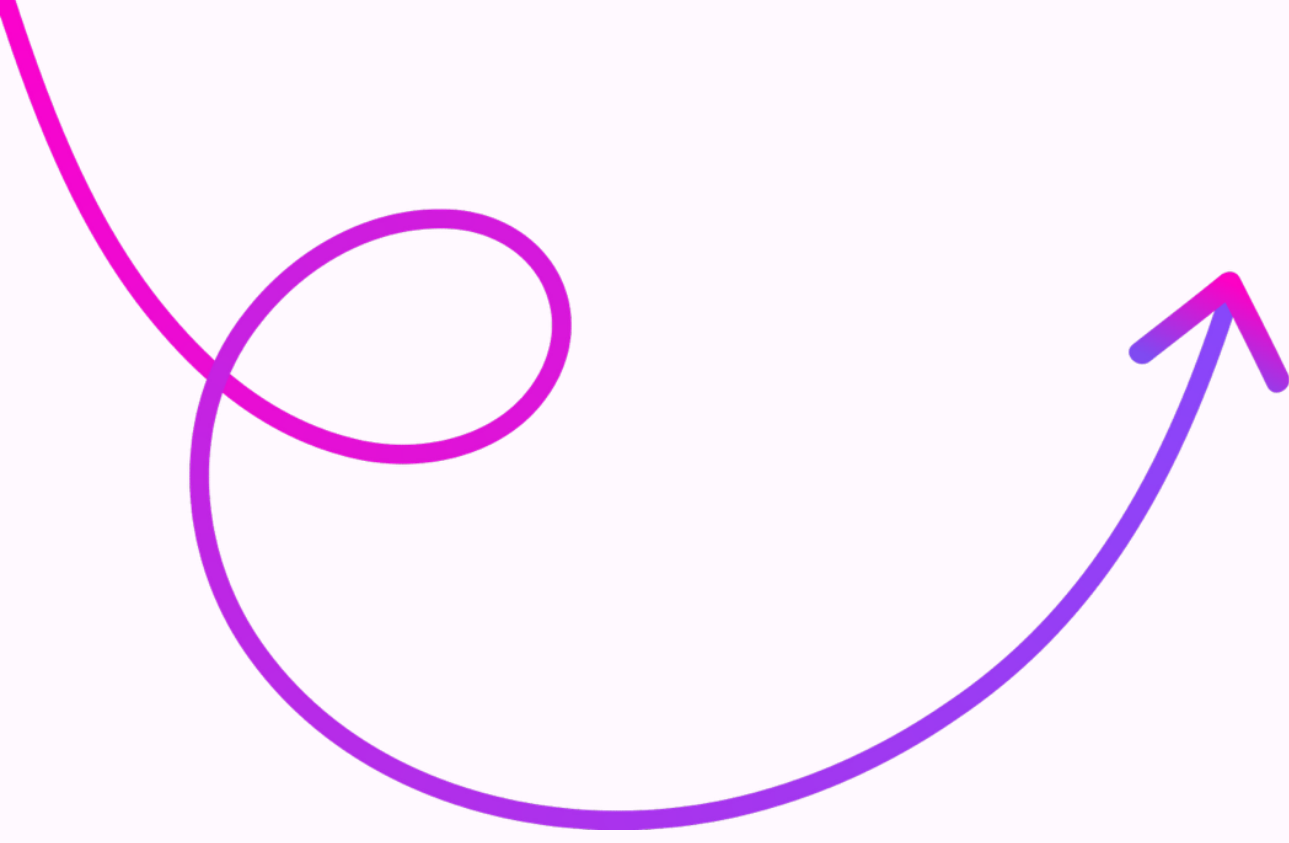




Data Protection Impact Assessment

Juniper Intelligence

Date: 29/07/2026

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.

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.

Juniper Intelligence is a new product, live since 1 September 2026. It reviews data a school already holds in Juniper products and presents a short, ranked list of Indicators: plain-language findings, each backed by the underlying evidence. At launch it draws on Sonar Tracker and Sisra Analytics; further Juniper products are planned.

It is being introduced because patterns in a school's own data can be missed when staff have to run the analysis manually. The objective is to bring those patterns to the attention of the staff who need them, and over time to help schools turn them into action.

Indicators support professional judgement; they do not make decisions about pupils. Whether and how to act stays with the school.

Indicators are produced deterministically: a catalogue of defined checks is run over a copy of the school's data, and each finding is presented as a pre-written sentence with the school's own figures inserted. No AI model is used and no personal data is sent to any AI provider.

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 innovative 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 below then complete Part 2 of this form.

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

Date of DPIA Screening	29/07/2026
Result of DPIA Screening	Full DPIA required

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):

These categories reflect the personal data available across the Juniper products that may feed Juniper Intelligence. The categories used at launch are set out under Nature and context of the processing.

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.

Customer (establishment/school staff); Pupils in school; Pupils' parent(s)/guardian(s).

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, customers contract Juniper to provide technological services and would expect this. Juniper customers will need to consent to their data being processed through Intelligence before Indicators are displayed.

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 purpose of the processing is to get the right information to the right person at the right time. Juniper Intelligence surfaces findings from data a school already holds, so that patterns which might otherwise be missed are brought to the attention of the staff who need them, without the school having to run the analysis manually.

The processing does not create new categories of personal data. It applies defined checks to data the school has already provided to Juniper through its existing products, and presents the result in plain language.

Data is also used to check and improve the accuracy and reliability of the Indicators provided to the school, as set out in the activation terms. It is not used to train AI models.

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?

Juniper Intelligence is the responsibility of Product and Engineering. Juniper will benefit commercially and technically. Customers will benefit from improved technology and processes, and be able to work more effectively and efficiently by surfacing insights which may otherwise be missed.

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.

Juniper customers activate Juniper Intelligence to generate Indicators from data already held in Sonar Tracker or Sisra Analytics (and other Juniper products in future iterations). Activation and consent is by the school's existing Account Owner/Admin.

Juniper Intelligence does not collect new personal data. It uses data that Juniper already processes on the school's behalf through its other products, under the school's existing agreements with Juniper, for the additional purpose of generating Indicators.

On activation, data from the source product is copied into a separate Juniper Intelligence database held by Juniper. Indicators are generated by running a catalogue of defined checks over that copied data. Each finding is rendered as a pre-written sentence with the school's own figures inserted; no free-text generation is involved.

The free tier names no pupil. The paid Evidence tier shows the specific pupils behind a finding.

Data is copied from the source product into the Intelligence database by a synchronisation process, which updates existing records in place rather than accumulating a history. Synchronisation and Indicator generation run automatically on a daily schedule.

The data copied from Sonar Tracker comprises pupil identity (name, UPN and date of birth), year group, gender, assessment and attainment data, attendance figures, SEN status, free school meals and pupil premium eligibility, EAL status and first language, ethnicity, and other contextual flags such as looked-after, service child and disadvantaged status. Behaviour, exclusions, contact details, addresses, next of kin, medical and dietary data are not copied from Sonar Tracker.

The data copied from Sisra Analytics depends on what each school has uploaded to Sisra. Alongside pupil names and attainment and results data, Sisra holds pupil attributes that the school defines and uploads itself, and these are copied as they are. Juniper cannot guarantee their content: depending on the school's own use of Sisra, they may include, for example, attendance information in banded or raw form, or other categories of personal data.

SEN status and ethnicity are special category data under Article 9 of the UK GDPR. Pupil attributes copied from Sisra may include further special category data, depending on what the school has uploaded.

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 Intelligence is a Laravel application deployed and managed through Laravel Cloud, a managed platform operated by Laravel Holdings Inc., with its own database holding data copied from connected Juniper products. These are Sonar Tracker and Sisra Analytics, with Juniper Portal providing subscription state and user administration. Customers control which of their connected systems are made available to Intelligence and can disable data sources at any time.

Data is transmitted over secure connections and processed solely to generate Indicators; it is not used for any other purpose. Access is governed by authentication, role-based permissions and product-level authorisation controls.

No personal data is sent to any external AI provider.

The application runs on Amazon Web Services infrastructure in eu-west-2 (London). Its database is a Laravel Serverless Postgres cluster, operated for Laravel by Neon, also on AWS in eu-west-2. Web traffic to the application is served through Laravel Cloud's edge network, which is operated by Cloudflare. Pupil data is stored and processed in the UK. Error monitoring is provided by Sentry, hosted in the EU region, which is covered by the UK's adequacy regulations; error reports do not contain pupil data. Wonde has no direct connection to Juniper Intelligence: where a school uses Wonde, data flows from Wonde into Sonar Tracker or Juniper Portal, and reaches Intelligence only through synchronisation from those products.

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
Laravel Cloud	Application platform: deployment, operation and database. Laravel Cloud uses Amazon Web Services for infrastructure, Neon for the database and Cloudflare for its edge network.	UK (AWS eu-west-2, London). Edge traffic is handled by Cloudflare's global network.	Privacy Policy - Laravel Cloud
Sentry	Application error monitoring. Error reports do not contain pupil data.	EU	sentry.io/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.

Yes, Product and Engineering has consulted with internal stakeholders and will seek additional views as part of normal feedback, review and development.

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

Juniper Executive, Security and Compliance, and IT Teams have been consulted.

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?

Data within Juniper Intelligence belongs to Juniper customers; they are the Data Controller and responsible for rights requests. Juniper will assist with these on request in its capacity as Data Processor.

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, and Juniper is the Data Controller, what is the lawful basis for processing the special category data?

Note: only complete this section where Juniper is the Data Controller. Where the Juniper customer is the Data Controller, it is their responsibility to ensure they have a lawful basis or bases for processing 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?

Data will not be shared or otherwise processed other than for the contracted purposes.

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?

Customers can control what data is shared with Juniper Intelligence and are responsible for the outputs from it.

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?

All data used by Juniper Intelligence comes from existing Juniper products. Customers have responsibility for ensuring the data in these products is accurate.

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?

Juniper will process data for the contract term, up to 8 years.

Juniper Intelligence holds its own copy of school data, in a separate database, in order to generate Indicators. Synchronisation updates that copy in place rather than accumulating a history of it.

Generated Indicators have no separate expiry. They persist for the duration of the contract, so that an Indicator raised for a cohort can be tracked across terms and years and remains available at a stable link.

When a school deactivates Juniper Intelligence, its Indicators are hidden immediately and no new Indicators are generated. Data is deleted within 90 days of deactivation, and within 90 days of contract termination. Records deleted in the source system are already excluded from Indicators.

Juniper Intelligence also holds personal data about the school staff who use it: names, email addresses, login session records, preferences, and records of consent and purchase. This is retained for the contract term and deleted on the same basis.

Application and access logs are retained by the hosting platform for 7 days. Database backups are retained for 7 days with point-in-time restore; data deleted from the live database may therefore persist in backups for up to a further 7 days before ageing out.

Security

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

Juniper Intelligence is developed and operated in accordance with Juniper's Information Security Management System (ISMS), which is certified to ISO 27001. Juniper applies secure development lifecycle practices, security testing, change management processes, access controls, vulnerability management and supporting information security policies to protect the confidentiality, integrity and availability of customer data.

Juniper Intelligence is an optional feature and is not enabled by default. Customers may choose whether to activate the service, even where it is included within their subscription. Prior to activation, customers are presented with appropriate warnings, guidance and usage information and must accept the terms before the feature can be enabled.

Customers can subsequently revoke this consent and disable the service at any time.

Activation of Juniper Intelligence is restricted to users with appropriate administrative permissions within supported Juniper products. At present, the feature can only be enabled by users with Account Owner or Account Admin permissions within Juniper Portal. This capability may be expanded to additional Juniper products in the future.

Juniper Intelligence holds data from multiple schools within a single database. Separation between schools is enforced in the application layer: queries are scoped to the school identified from the authenticated session or a verified token, never from user-supplied input. A dedicated automated test suite covers cross-school access, including attempts to spoof a school identifier and planted collisions between pupil identifiers in different schools. Database-level row-level security is designed into the table structure and is a planned addition, providing defence in depth behind the application-level controls.

All access to Juniper Intelligence is performed over secure authenticated connections. Access to generated Indicators is governed by the permissions and role-based access controls applied within the relevant Juniper products. Customer data remains under the control of the customer as Data Controller, and customers determine which data is made available to Juniper Intelligence for processing.

Juniper Intelligence is deployed and managed through Laravel Cloud, which holds SOC 2 Type 2 attestation for Security, Confidentiality and Availability, and ISO 27001 certification. The application runs on AWS in eu-west-2 (London), and its database is Laravel Serverless Postgres, operated by Neon on AWS in eu-west-2. Data is encrypted at rest and in transit by the platform, and database connections require TLS. Traffic to the application passes through Cloudflare's edge network, which filters common injection, authentication and data-exposure attacks before they reach the application. Database backups are retained for 7 days, with point-in-time restore available within that window.

Application errors are reported to Sentry, hosted in the EU region. Error reports are configured so that they do not contain pupil identifiers, names or attainment data, and Sentry's collection of default personal information is disabled.

Future Developments

Use of AI and a large language model (LLM), via Amazon Bedrock in a UK region, to produce written narrative that explains and contextualises the figures, and to help schools draft action plans and school improvement plan objectives.

Scope and Review Triggers

This DPIA must be reviewed and re-approved before any of the following takes effect:

- a new category of personal data is made available to Juniper Intelligence, including through a change to the permissions a school grants;
- Indicators are generated using special category data not already within this scope;
- processing moves from surfacing data a school already holds to predictive or profiling output about identifiable individuals;
- a new interface materially changes how users interact with personal data through the product;
- Juniper Intelligence is extended to a further Juniper product, or a further sub-processor is introduced;
- output is used for a purpose other than generating Indicators and the evidence supporting them;
- there is a material change to hosting location or sub-processor arrangements.



Juniper
Education

Junipereducation.org

© 2026 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.