Portal Data Protection Impact Assessment

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.

d

Juniper Portal is a new product intended to serve as the central hub that controls access to and relays data to and from other Juniper Products.

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.

Date of DPIA Screening	07/08/2025
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 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. 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.

Customers (establishment/school staff); Pupils in school; Pupils' parent(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.

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 processing is to allow users to manage staff, pupil and parent records, to send out invitations to new staff and parents as well as managing certain school information (key contacts, school improvement plan etc.)

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?

Portal is the responsibility of Product and Engineering. Juniper will benefit commercially and technically. Customers will benefit from improved technology and processes.

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.

Subjects will have their data collected and organised into relevant data storage. This will encompass everything that allows the user to work with the subject, such as identity and contact details. The data will come directly from our MIS or via Wonde.
Data is stored in secure cloud storage services. Processing occurs on a real time or scheduled basis. Data that is processed will then be available in the system to view so that users can make any interventions required.

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.

Data is being stored in AWS data centers in London region. The AWS services used are:

- EC2 instances – web servers and compute
- Aurora RDS – data base
- Redis – cache, sessions, asynchronous queues
- RabbitMQ – internal messaging between the Juniper Services
- CloudWatch – stores application logs
- DMS – used to synchronize DB data in different RDS instances
- FusionAuth – enterprise grade service used for user authentication

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	To enable data sharing between school services.	UK	Privacy policy - Wonde
AWS	Hosting	UK	AWS Privacyd

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.

Juniper 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?

Group Data Protection Officer and Group Information Security Officer.

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 Portal 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, 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?

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?

Ultimately customers can control what data is shared with Juniper. The data comes from trusted sources controlled by customers.

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?

Customers have responsibility for ensuring the data is accurate.

Storage Limitation (Retention)

What is the retention period for the various types of personal data? If you cannot specify a specific retention periods, 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 agreed period of the contract up to a maximum of 8 years. On termination of the contract, data will be delieted within 90 days.

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 is used as service provider. AWS computing environments are continuously audited, with certifications from accreditation bodies across the world. AWS blocks all traffic by default; access is managed via Security Groups and Least Privilege access control. Default AWS threat detection and prevention mechanisms in place. AWS inbuilt BC/DR features in use with multiple availability zones.

All API calls are authenticated with secure tokens and transmitted on a secure SSL connection. Configuration is effectively managed by dedicated third-party.

Data is encrypted at rest and in transit.
Access is controlled via login, 2FA and SSO.
Passwords are encrypted with Bcrypt.
Daily backups are kept and there is 20-day period in which the main database can be restored to any point in time.
Changes undergo peer-review before being implemented.
Logging is enabled for some processes and Monitoring is conducted as required.
Planned penetration testing and regular vulnerability assessment.

Juniper

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

Junipereducation.org