Data Protection Impact Assessment

People First
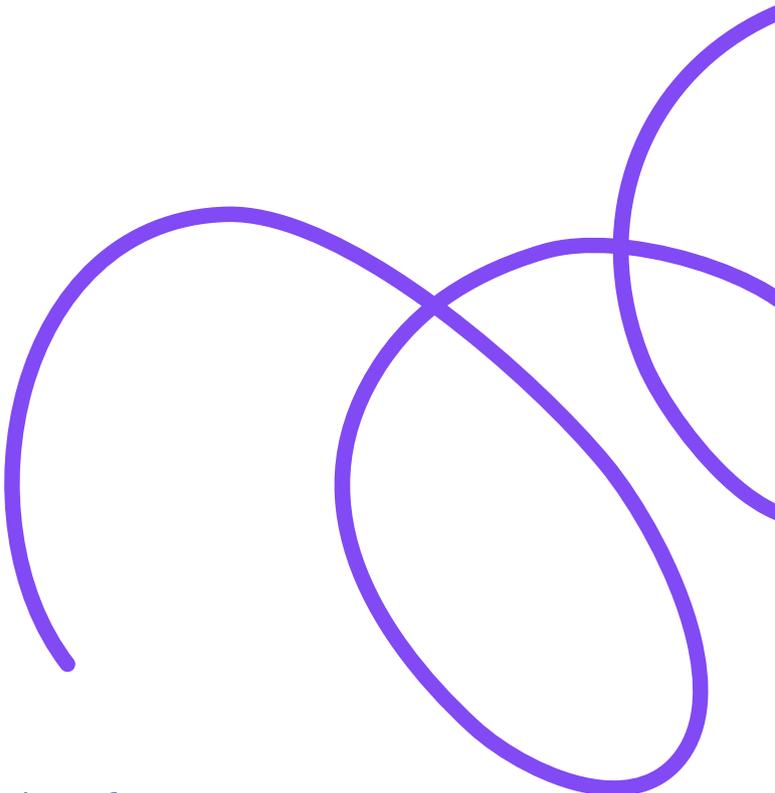
Date: 01/07/2025

Juniper

Contents

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

enquiries@junipereducation.org   0345 200 8600   Junipereducation.org

Juniper

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.

> In order to provide HR software to customers, Juniper Education will resell the People First software provided MHR Global, MHR Campus, Mere Way, Ruddington, Nottingham, NG11 6JS, https://mhrglobal.com/
>
> Juniper will also use MR HRIS and Payroll solutions for internal business functions including pension data and admin solutions.

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	02/07/2025
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):

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 data subjects whose personal data is being processed include:
- Employees and former employees, contractors of Juniper
- Employees of schools and trusts, including teaching and support staff
- Senior leaders and HR/payroll administrators who access or manage the platform
- Casual, temporary, and supply staff engaged by schools
- Former employees, for whom limited data may be retained for statutory or payroll purposes
- Emergency contacts/next of kin nominated by employees
- Occasionally, job applicants or new starters, where onboarding data is entered in advance

The relationship between Juniper and the data subjects is both direct and indirect, as Juniper acts as a data controller for its own employee data and as a data processor on behalf of its school and trust customers, who are the data controllers. The primary service being delivered is HR and Payroll processing, with some customers using the full self-service HRIS functionality and others relying solely on the bureau service managed by Juniper.

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, the individuals whose data is being processed would reasonably expect their personal data to be used in the ways envisaged. The processing of personal data within the People First (JHRIS) platform is in line with standard employment practices and is necessary for:
- Administering salaries, pensions and statutory deductions
- Managing employment records (e.g. contracts, job roles, leave)
- Ensuring statutory compliance (e.g. HMRC reporting, pensions, workforce census)
- Facilitating internal processes such as absence management, performance tracking, and communication

These uses are clearly connected to the employment relationship and are typically outlined in contracts of employment, staff handbooks, and school privacy notices. Where special category data is processed (e.g. health or union membership), this is also within reasonable expectations for payroll or HR compliance purposes.

As Juniper acts as a data processor, customers (schools/trusts) are responsible for ensuring that their staff are informed about how their data will be processed. The processing aligns with the purposes disclosed to data subjects in the controller's privacy notices.

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 includes management of Juniper employee payroll data;

Supporting accurate, secure, and efficient delivery of HR and Payroll services for school and trust staff through the People First platform. Juniper acts as a data processor on behalf of schools, who remain the data controllers.
The organisation seeks to:
- Ensure timely and accurate payroll processing
- Maintain comprehensive and up-to-date employment records
- Facilitate statutory compliance (e.g. HMRC, pensions, census submissions)
- Enable improved data accuracy and auditability through system-driven workflows
- Offer enhanced self-service capabilities for employees and managers
- Reduce reliance on manual email/excel-based change submissions

How the Processing Differs from Previous Use
There are two main scenarios where data is pre-existing but the processing is changing:
1. Legacy Bureau Customers (Catalyst):
   o These schools were already using Juniper's legacy platform (Catalyst) for HR/Payroll processing.
   o The purpose of processing remains the same, but with People First, data is handled via a modern, cloud-based platform.
   o The shift enables more secure, auditable workflows and introduces greater self-service functionality, reducing the volume of change requests submitted via email or spreadsheet.
2. New Bureau Customers or SaaS-to-Bureau Conversions:
   o Some schools are new to Juniper's bureau service, or previously used Catalyst in a self-managed SaaS capacity.
   o These customers are now moving to a fully managed service where Juniper processes payroll on their behalf using People First.
   o This represents a shift in the role Juniper plays – from providing software alone to becoming a data processor handling payroll delivery end-to-end.
   o In these cases, Juniper will have increased access to staff data for the purposes of delivering the managed service, but processing remains aligned with the employment relationship and customer expectations.
In both scenarios, the processing stays within the original lawful purpose of managing staff employment and remuneration. The change primarily improves efficiency, control, and user experience.

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?

Responsibility for the processing:

Juniper Education takes responsibility for the secure and compliant processing of data within the People First (JHRIS)platform under its role as a data controllrt and processor.

Within Juniper:
- The Payroll Bureau and HR Services teams are directly responsible for handling and processing the data to deliver the service.
- The Product & Proposition team ensures the platform is configured and supported in line with customer needs and data protection requirements.
- The Data Protection Officer (DPO) oversees data protection compliance across the organisation, including third-party systems.
- Juniper's Information Security and IT teams support system integrity, user access controls, and data protection protocols.

Beneficiaries of the processing:
- **Schools and Trusts (Customers):**
  - Gain a more efficient and compliant HR/payroll service
  - Reduced manual administration and lower risk of payroll errors
  - Improved reporting, audit trail, and workforce insights
  - Stronger governance and easier fulfilment of statutory duties
- **Juniper Education:**
  - Improved service delivery efficiency and standardisation
  - Reduced operational risk from email- or spreadsheet-based processes
  - Stronger platform proposition with modern capabilities
- **School Employees (Data Subjects):**
  - Easier access to personal information and documents (e.g. payslips, absence records) via self-service
  - More timely and accurate payroll and HR processing
  - Greater confidence in data security and transparency of how data is handled

Intended effects on individuals:

The intended effects are positive. Employees will benefit from:
- Increased visibility of their data
- Faster resolution of payroll or HR queries
- Reduced errors and rework from manual submissions
- More secure handling of personal information

The system and service changes are designed to support a modern, professional experience for staff while improving data integrity for the employer.

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.

The processing involves the **collection, storage, use, and ongoing management of employee data** for the purpose of delivering HR and Payroll services to schools and trusts via the **People First (JHRIS)** platform, provided and supported by Juniper Education.

How Data is Collected

Data may be collected in one or more of the following ways:

- Directly inputted by the school/trust via the self-service portal
- Transferred securely to Juniper by authorised school contacts using agreed file formats (e.g. onboarding spreadsheets, secure email)
- Imported from legacy systems during system migration (e.g. Catalyst)
- Entered or updated by Juniper staff, based on instructions received from the customer
- In some cases, employees may enter or update their own data via self-service (e.g. contact details, leave requests)

How Data is Used

The data is used by Juniper staff to:

- Calculate and process payroll including statutory deductions (e.g. tax, NI, pensions)
- Manage employee records such as job roles, salaries, benefits, absences, and contract terms
- Support the generation of statutory and operational reports (e.g. payslips, workforce census, pension returns)
- Provide HR workflow support, such as recording appraisals or managing leave
- Respond to payroll or HR queries raised by the school or employee
- Manage pension data

Schools may also use the system for:

- Reviewing staff records and approving workflow requests
- Managing compliance-related HR tasks
- Accessing reports and dashboards for workforce management

How Data is Stored

- All data is stored securely within the People First cloud platform, hosted by MHR.
- Access is role-based, with strict user permissions managed either by Juniper or by the customer depending on the configuration.
- Juniper ensures appropriate data protection measures are in place, including encryption, audit logging, and secure data transfer protocols.

Scale, Size, and Frequency of Processing

- The processing occurs on a **continuous and cyclical basis**, with key peaks around monthly payroll processing, reporting deadlines, and start-of-term onboarding periods.
- Juniper supports hundreds of schools, meaning the **volume of data processed is significant**, encompassing thousands of employee records.
- Updates and interactions may occur daily, particularly where self-service is enabled.

Who Will Use the Information and Why

The following groups will access and use the data processed within the People First platform:

- **Juniper's Payroll and HR Services teams** – To carry out payroll calculations, pensions, manage employee records, handle statutory reporting, and respond to customer instructions and queries.
- **Authorised School or Trust Administrators** – Typically HR, finance or office staff who will manage and maintain employee data, approve changes, and run reports for operational and compliance purposes.
- **Line Managers (within schools/trusts)** – Will use the system to:

Juniper

- o Log and approve absences (e.g. sick leave, annual leave)
        - o Review and approve expense claims
        - o Participate in HR workflows such as appraisals or probation tracking
        - o View team-level workforce information where permitted by role-based access
- **Employees (school staff)** – Will use the self-service portal to:
        - o View payslips, P60s, and other personal documents
        - o Update personal details (e.g. address, contact info)
        - o Submit leave and absence requests
        - o Record and submit expense claims (where enabled)
- **System Administrators (Juniper and MHR)** – Will access the system for configuration, troubleshooting, updates, and auditing, all under strict access controls.

Novel Aspects of the Processing
- While the overall purpose of HR and payroll processing is well-established, the **use of the People First platform introduces a more modern, integrated approach** to handling this data:
        - o Increased self-service by employees and line managers
        - o Workflow automation that reduces email-based change requests
        - o Enhanced auditability and data accuracy
- For customers previously using Catalyst or non-integrated tools, this represents a **significant improvement in transparency, user experience, and data governance**.

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.

People First is provided MHR Global and is hosted in Microsoft Azure within a UK data centre.
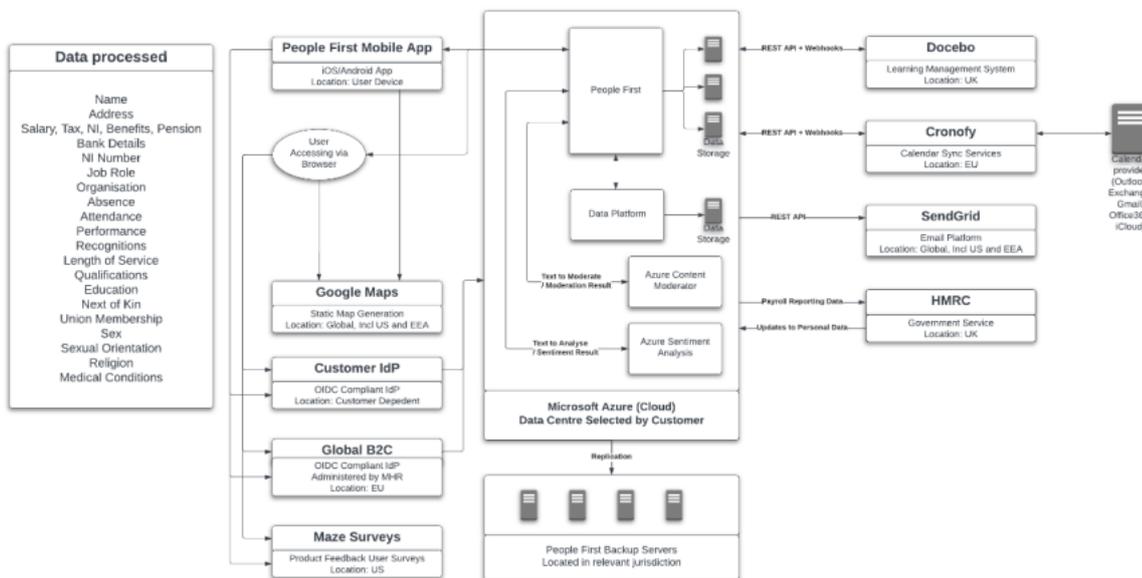
The data platform utilises an instance of Data Bricks hosted on the MHR Azure tenant.

Notes on services referenced above:

Global B2C – A service used to broker authentication to external Identity Providers (e.g. Google/Facebook). Requests profile and email scopes (giving access to basic information like user's name, picture, and email address) run through Microsoft Azure.

Google Maps – A third party service used to generate a static map showing a location based on geographic co-ordinates. This is used as part of the Employee's profile to show the location of their address.

Azure Content Moderator – An Azure service that is used to moderate text for the presence of profanities. No data is persisted by the service once the request has been processed.

Azure Sentiment Analysis – An Azure service that is used to process text and extract sentiment. No data is persisted by the service once the request has been processed

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
MHR Global	Software Provider	UK	https://mhrglobal.com/uk/en/privacy-policy
MHR Pension Data Solution	Software Provider	UK	Data Controller Instructions PENSION DATA SOLUTION December 2024.pdf
MHR Pension Admin Service	Software Provider	UK	Data Controller Instructions PENSION ADMIN SERVICE December 2024.pdf
Cronofy	Mail/calendar integrator	EU	Privacy Notice	Policies	Cronofy Docs
Twilio Send Grid	Email service	EU	Website Privacy Notice	Twilio
Microsoft Azure	Hosting and related services	UK & EU	Data Privacy in the Trusted Cloud	Microsoft Azure
Google Maps	Identifies location	US	https://mapsplatform.google.com/
HMRC	HM Revenue & Customs	UK	HMRC Privacy Notice - GOV.UK (www.gov.uk)
Maze	Product feedback and surveys	US	Privacy policy - Maze (mymaze.com)

The following optional services are available to customers.

Name	Purpose of processing	Country	Privacy Notice Link
Broadbean	Job posting	UK	Talent Attraction & Acquisition Software	Broadbean UK
eQuest	Job posting	UK	Privacy Statement - eQuest
Sovren	CV parsing	EU	Privacy Statement	Textkernel
Docebo	E-learning system	UK	Docebo - Privacy Policy - Docebo
Rustici	E-learning content	UK	Privacy Notice - Learning Technologies Group plc (ltgplc.com)

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, a level of consultation has taken place with key stakeholders to support transparency and ensure the processing meets user expectations.
>
> Juniper engaged with selected school and trust staff during the development and onboarding phases of the new People First (JHRIS) solution. Demonstrations of the system were provided to:
> - Key administrative users (e.g. HR and payroll staff)
> - Representatives from multi-academy trusts (MATs)
> - Internal service teams delivering the payroll bureau function
>
> These sessions allowed stakeholders to view the new functionality, understand how data would be processed, and provide feedback on usability, configuration, and access requirements (e.g. for line managers or employee self-service).
>
> Given that the processing purpose remains consistent with existing employment-related services, and that the platform enhances transparency and control over staff data, a broader public or end-user consultation was not deemed necessary at this stage.
>
> Customers remain responsible for updating their own privacy notices and communicating any changes to their staff, as data controllers.

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

> To ensure that all potential risks associated with the envisaged data processing are fully understood and appropriately mitigated, Juniper Education has engaged with the following internal stakeholders:
> - **Data Protection Officer (DPO)** – Provides guidance on GDPR compliance, data minimisation, lawful bases for processing, and ensures that appropriate controls are in place for the handling of personal and special category data.
> - **IT & Information Security Teams** – Responsible for reviewing system architecture, integrations, user provisioning, access controls, and vendor assurances. They ensure that data is stored and processed securely, using appropriate encryption, audit logging, and technical safeguards.
> - **Service Delivery and Operations Leadership** – Including Heads of HR Services and Payroll, who ensure operational processes are secure, efficient, and aligned with data protection obligations.
> - **Product & Proposition Team** – Assesses how system design and configuration choices impact data flows, user access, and service delivery, helping to embed privacy by design principles.
> - **Executive Leadership and Board** – The Board is kept informed of significant changes involving data processing, particularly where these relate to customer experience, reputational risk, or regulatory compliance.
>
> This cross-functional approach ensures that data protection is embedded into the implementation and ongoing management of the People First platform.

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?

Juniper customers will be responsible for dealing with rights' requests from data subjects whose data is processed within People First, as part of the contracted services provided by Juniper. This is because the customer (e.g. the school or trust) is the Data Controller and therefore holds responsibility for fulfilling obligations under data protection legislation. Juniper acts as a Data Processor and will support the customer in responding to rights requests where required, in accordance with the terms of the Data Processing Agreement and applicable law. This may include retrieving, correcting, or deleting data at the customer's instruction.

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?

Fields within the People First platform are configured to support the management of employees and organisational structures, ensuring that **only the personal data necessary for the delivery of HR and Payroll services is collected and processed**.

Where specific data is **not required**, the **Custom Card** used to collect it can be hidden, preventing unnecessary data collection. This allows the system to be tailored to each organisation's needs, ensuring data minimisation is applied by default.

Conversely, **Custom Cards can also be added** where a customer has a legitimate need to collect additional information relevant to their organisation. These controls help ensure that data processing remains limited to the documented and intended purposes outlined in this DPIA.

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 are in control of the data provided for processing. The People First platform supports this by allowing customers to determine which data fields are used, required, or hidden, depending on their organisational and statutory needs.

This flexibility ensures that only adequate and relevant information is collected and processed, and that it is limited to what is necessary to achieve the agreed HR and payroll service outcomes. Juniper does not collect or process additional data beyond what is instructed by the customer in line with their role as Data Controller.

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 are in control of the data provided for processing and are responsible for ensuring its accuracy. As Data Controllers, schools and trusts must ensure that the personal data they input or instruct Juniper to process is accurate and kept up to date, in line with their obligations under UK GDPR.

The People First platform supports data accuracy through:
- Self-service access for employees, allowing them to view and update key personal details (e.g. address, contact information)
- Automated validation of certain fields during data entry (e.g. NI numbers, bank details)
- Clear audit trails and change logs, supporting transparent record management

Failure to keep data up to date may result in negative consequences, including:
- Incorrect salary payments or deductions
- Failed bank transfers
- Inaccurate reporting to HMRC or pension providers
- Delays in responding to employee queries or statutory submissions

As a Data Processor, Juniper processes data as instructed and relies on customers to provide timely and accurate updates to ensure service quality and compliance.

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?

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

Juniper

The People First software allows for the application of retention schedules. At present this is a manual process. There are developments planned that will allow for records to be identified, reported and removed or retained as part of a scheduled task.

Juniper will only process data for the minimum period necessary to provide the contracted services and meet with legislative requirements.

Security

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

People First Tech Security Solution Sheet.pdf (mhrglobal.com)

Juniper

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

Client: Name Here

Junipereducation.org