



Data Protection Impact Assessment



Juniper Communications Hub

Date: 28/09/2026



Juniper

Contents

Data Protection Impact Assessment (DPIA)3

 How to complete a DPIA3

 Screening.....3

 Full DPIA Assessment.....3

 Part 13

 DPIA Screening3

 Part 25

About the Processing5

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.

Juniper Comms Hub is cloud-based parental engagement system, designed for schools, comms hub transforms school communications by providing a unified user interface for all communication methods, contributing to optimised message delivery whilst keeping costs low.

Unlike other school communication platforms, our system will transform school communication into strategic, omni-channel communications and will contribute to enhanced parental engagement.

Customers can use comms hub to send email, SMS and app messages. News, newsletters and events flow through comms hub to the app for website customers.

It is a new product, that Juniper will use to accompany our new MIS as well as other products in the Juniper eco-system.

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

Result of DPIA Screening	Full DPIA required / Full DPIA not 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):

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.

Juniper Comms hub holds information on staff, pupils and parents.

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.

The subjects 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 processing allows users to effectively send content or communications to recipients to keep them informed about their child and wider school news.

Twilio (SMS Message Delivery)

Purpose and business need: Twilio is used exclusively to fulfil the core Comms Hub function of enabling schools/establishments to send time-sensitive SMS communications to parents, carers and staff.

AWS Simple Email Service (Email Message Delivery)

Purpose and business need: AWS SES underpins the email communication channel of Comms Hub, allowing establishments to reach recipients via email-based communication.

Integration with Events

Purpose and business need: This integration allows Comms Hub to provide a single, unified view of school communications and school events to parents, carers, and staff, avoiding the need for users to consult a separate system to understand event context referenced in a communication, and supporting the core purpose of Comms Hub as a consolidated communications and engagement platform.

Integration with Websites

Purpose and business need: This integration ensures that news, newsletters and events published publicly on an establishment's website are also visible to parents, carers, and staff within Comms Hub and the Juniper Education App, reducing duplicate data entry for establishments and providing a single point of reference for school communications regardless of where the event was originally created.

Integration with Mobile App

Purpose and business need: This integration extends the reach of Comms Hub's core communication functions to a mobile-first channel (app messaging), meeting the expectation of parents and carers for timely access to school communications on their personal devices, and supporting time-sensitive use cases where immediacy of access is important.

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 will benefit commercially and in relation to product development through feedback. The user will benefit from the processing as it will allow them to engage and communicate parents. Increasing parental engagement improves outcomes for children.

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. Data is collected via Portal and passed to the Comms Hub product. The data between the schools MIS and Portal is synchronised daily. However, there is an instant sync between Portal and Comms Hub. Content and data also syncs on refresh between Comms Hub and the Mobile App.

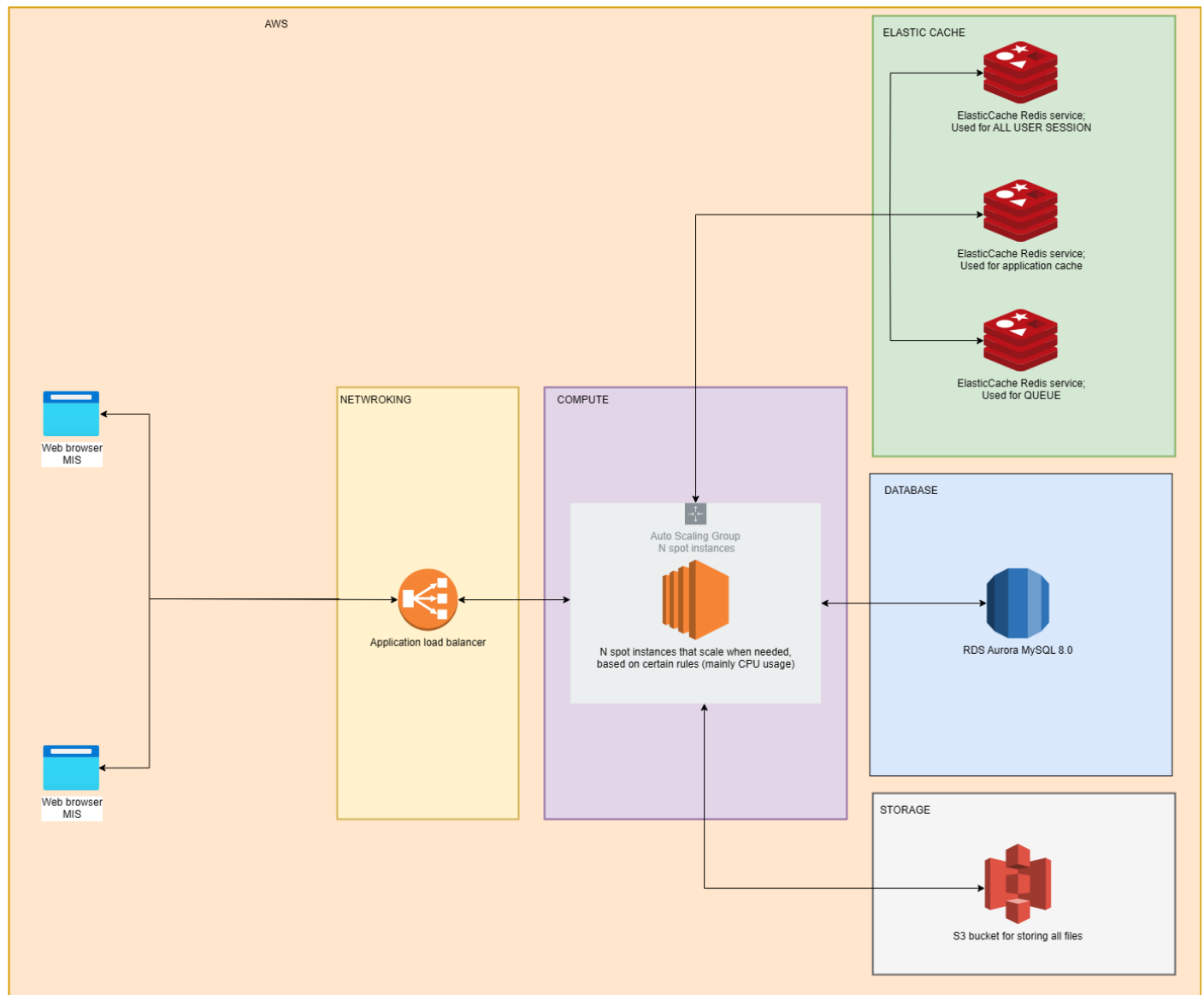
Data is stored in secure cloud storage services. Processing occurs on a real time or scheduled basis. Data that is processed will then be available in the system to view so that users can make any interventions required.

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.

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



Comms hub

The Comms hub 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

Database - RDS Aurora

Storage - S3

ETL Tooling

The ~~ETH~~ 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

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
AWS	Hosting	UK	Link
Twilio	Sending SMS	USA	Link
AWS Email service	Sending Emails	UK	Link
FusionAuth	User authentication	UK	Privacy Policy - FusionAuth

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.

No, the organisation has a similar product with customers and they expect this level of processing.

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?

~~Data within Comms Hub~~ 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?

The data is only shared with the organisation or 3rd parties on their behalf, any related technical products have agreements in place to ensure GDPR requirements are met.

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

~~we look after you, so that you can look after our children~~

~~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?

There is a limited data set that can be processed and this is all viewable in the product. The Comms Hub 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?

Data in comms hub will always come from our MIS, another MIS. Those products will always be the single point 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?

Data is retained for the contract length up to a maximum of 8 years. On termination of the contract, data is destroyed 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 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 Comms Hub 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.

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

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.

Twilio (SMS Message Delivery):

- All communication with the Twilio API occurs over TLS-encrypted HTTPS connections.
- Inbound webhook callbacks from Twilio (delivery status updates) are authenticated using Twilio's X-Twilio-Signature header, which is cryptographically validated against the shared Twilio auth token before any payload is processed; requests failing signature validation are rejected with an HTTP 403 response.
- Only the minimum data necessary for message delivery (recipient phone number and message body) is shared with Twilio; no additional data beyond what is required for the specific communication is transmitted.
- Twilio acts as a data processor under a data processing agreement and does not retain message content beyond its own operational and legal retention requirements.

AWS Simple Email Service (Email Message Delivery):

- All communication with AWS SES occurs over TLS-encrypted connections, and access to the SES API is authenticated via scoped AWS IAM credentials restricted to the SES/SNS actions required.
- Inbound delivery and bounce/complaint notifications are received via dedicated webhook endpoints, with request authenticity verified before processing.
- AWS SES operates within Amazon's shared responsibility security model and is covered under AWS's data processing terms; email content and recipient data are processed only for the purpose of transmission and are not used by AWS for any secondary purpose.
- A dedicated SES configuration set is used to isolate and track Comms Hub's sending reputation and delivery events separately from other services.

Integration with Events:

- All API requests between Comms Hub and Events are authenticated using OAuth 2.0 client-credentials JWT bearer tokens, issued and scoped by the organisation's identity provider (FusionAuth), with each token limited to a specific audience and read-only scope appropriate to the data being retrieved.
- Access tokens are short-lived, cached, and automatically refreshed/rotated on expiry or on receipt of a 401/403 response, minimising the exposure window of any individual credential.
- All API traffic is transmitted over TLS-encrypted HTTPS.
- Only event/calendar metadata required for display purposes (title, timing, location, description) is retrieved and stored in Comms Hub; no data flows in the reverse direction from Comms Hub to Events as part of this synchronisation.

Integration with Websites:

- API requests to Websites follow the same authentication approach as the Events integration: OAuth 2.0 client-credentials JWT bearer tokens scoped to a dedicated audience, issued via the organisation's identity provider, transmitted exclusively over TLS-encrypted HTTPS.
- Synchronisation retrieves only calendar/event data intended for public or establishment-wide display; no personal data relating to individual pupils, parents, or staff is exchanged as part of this integration.
- Tokens are subject to the same short-lived, automatically-rotated lifecycle as described for the Events integration, limiting the impact of any potential credential compromise.

Integration with Mobile App:

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

- End users authenticate to the Mobile App via the organisation's identity provider (FusionAuth), with single sign-on (SSO) issuing individually-scoped access tokens; authentication failures are handled through dedicated exception handling to avoid ambiguous or leaking error responses.
- Each API request from the Mobile App is authenticated using a per-user JWT bearer token bound to that user's identity and permissions; the API enforces the same establishment-level and role-based access controls as the Comms Hub web application, ensuring a mobile user can only retrieve data they are authorised to see.
- All traffic between the Mobile App and the Comms Hub API is transmitted over TLS-encrypted HTTPS.
- Authentication tokens are persisted and tracked (auth token records linked to the underlying identity provider user) to support token lifecycle management, including revocation, expiry, and refresh, reducing the risk associated with a lost or compromised device.



Juniper

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

Client: Name Here

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.

