Data Protection Impact Assessment

Juniper Websites

Date: 31/07/2025

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.

Data Processing Activities:

User Management: The CMS stores user login credentials (username and secure hash of password), identity information (title, name) and assigns roles/permissions for content management.

Content Management: Authorised personnel can create, edit, and publish content on the school website. This content may involve personal data in two ways:

- Indirectly: Content could include staff names, announcements with student achievements, or other information that identifies individuals.
- Directly: Schools may choose to capture personal data through website forms (e.g., contact forms, booking forms).

Wonde Integration (Optional): Schools can integrate with Wonde (MIS) to synchronise pupil data. The specific data synced depends on the permissions set by the school. For Add-ons to function correctly, there is specific data we require.

Access controls are in place to restrict access to personal data based on user roles and permissions.

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	31/07/2025
Result of DPIA Screening	Full DPIA required

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.

School Personnel:

- **Teachers:** Names, titles, and potentially profile photos for staff directories or department pages.
- **Governors:** Names, titles, and potentially profile photos for introductions or contact information.
- **Other Staff:** This could include office staff, IT personnel, or anyone with authorised access to the CMS. Contact details may also be imported from Wonde for use in the parents evening system and for emails/text messages. Their data might include names, titles, and potentially some contact information.

Students:

- **Names:** This could be included in announcements, group photos, award recognitions, or student work samples (depending on permission).
- **Attendance, academic, behavioural data, contact data (depending on Add-ons):** If the CMS integrates with a Management Information System (MIS), this data could be synced for parent portals.

Parents/Guardians:

- **Names:** Typically included for login purposes to a parent portal (if available) or when completing an online form, survey or poll.
- **Contact Information:** Email addresses or phone numbers might be stored for communication purposes.
- **Student Relationship:** This is used to link parents to their children's data within the CMS (e.g., parent portal).

Website Visitors (Limited Data):

- **IP Addresses:** Not directly linked to individuals.

Shop Customers (if available):

- **Account information:** Encrypted password.
- **Names:** Included for transactional purposes.
- **Contact Information:** Postal address, email address or phone numbers might be stored for transactional and communication purposes.

Alumni/Registration sign-up users (if available):

- **Account information:** Encrypted password.
- **Names:** Included for login purposes.
- **Contact Information:** Postal address, email address or phone numbers might be stored for communication purposes.

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.

School Personnel:

- Staff can reasonably expect their names, titles, and potentially photos to be used for staff directories, department pages, or contact information on the website. This facilitates communication and transparency within the school community.

Parents/Guardians:

- Parents can reasonably expect their names and contact information to be used for a secure login to a parent portal (if available) and for communication from the school.

Students (and Parents):

- Student names in announcements, group photos, or award recognitions: This can be expected to some extent. However, schools should clearly communicate their policy on using student names and obtain consent for situations where identification might be unexpected (e.g., using student work samples with names attached).
- Attendance, academic, behavioural data (through add-ons): Sharing this data through a parent portal is somewhat expected, but schools should ensure parents understand this practice and have a way to opt-out if needed.

Website Visitors (Limited Data):

IP Addresses: These are typically collected by default for website analytics; however, they are not directly linked to individuals.

Shop Customers (if available):

- Shop customers should anticipate that their passwords are securely encrypted. Using names for transactional purposes is necessary for order processing, confirmations and order updates. Schools should clearly communicate their policy on using customer names and contact data for transactional purposes.

Alumni/Registration sign-up users (if available):

- Users can expect their passwords to be encrypted to prevent unauthorised access. Names are necessary for identification and account management. Storing contact information is essential for communication. Schools should clearly communicate their policy on using sign-up usernames and contact data for communication purposes.

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?

Juniper Websites has a legitimate interest in using certain personal data to assist schools in fulfilling their educational mission and maintaining communication with staff, parents, and the broader community, in accordance with their service agreement as specified in the order confirmation. Schools should establish clear policies detailing how data is collected, used, and protected, and they should obtain consent from parents/guardians when processing student data beyond what is reasonably expected.

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:

- **Data Processors:**
    - Juniper Websites: CMS and Add-ons
    - Wonde (if available): MIS Data
    - MailGun (if available): Email delivery
    - ClickSend (if available): Text message delivery

Beneficiaries:

- **Juniper Websites:** Benefits include fulfilling contractual obligations with schools, improving the CMS based on usage data, and potentially offering additional data-driven services to schools.
- **Schools:** Benefits include a user-friendly platform for website management, improved communication with staff, parents, and the community, and potentially data insights for school improvement through anonymised web analytics.

Intended effects on individuals and their benefits:

- **School Staff:** Easier content creation and management, potentially improved communication with colleagues and parents.
- **Parents/Guardians:** Easier access to information and communication with the school through a parent portal (if available).
- **Students (if data is processed):** Improved learning experience through a well-maintained school website and communication channels.
- **Website Visitors:** An improved user experience on the school website with easy to find information.

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 Collection:

Data is collected through various means, including:

- **Synchronisation:** Integration with Wonde (MIS) to automatically synchronise pupil data. Calendar integration with Microsoft Outlook and Google.
- **Manual Input:** Authorised personnel manually input data into the school CMS.

- **Forms and Surveys:** Data collected from forms and surveys filled out by staff, students, parents, and visitors.

- **Booking systems (if available):** Data collected from booking systems e.g. club booking, filled out by parents.

- **Web Content:** Data included in website content, such as staff names, student achievements, and announcements.

Data Usage:

- **Communication:** Sending notifications and updates to parents, staff, and the community. Feedback to parents/guardians regarding a student's academic progress, and monitoring attendance.

- **Operational Management:** Scheduling events, coordinating staff activities, and managing visitor access.

- **Website Content:** Publishing information relevant to the school community, such as news, achievements, and important announcements.

Data Storage:

All personal data stored within the CMS environment is encrypted using industry-standard and secure encryption methodologies. This includes:

- **Encryption at Rest:** Data is encrypted when stored on servers, minimising the risk of unauthorised access in the event of a security breach.

- **Salting:** An additional security layer is implemented by salting passwords before hashing them. This further strengthens password protection.

- **No Plain Text Storage:** Juniper Websites ensures that personal data is never stored in plain text format. This significantly reduces the risk of compromising sensitive information.

Scale, Size, and Frequency of Processing:

- **Scale and Size:** The volume of data processed varies depending on the size of the school and the number of stakeholders involved (students, staff, parents, and community members).

- **Frequency:** Data processing occurs on a continuous basis, with regular updates through automated synchronisation, ongoing manual input, and periodic data collection through forms and surveys.

Users and Purpose:

- **Authorised Personnel:** Create, edit, and publish website content and communicate with parents/guardians.

- **Students and Parents/Guardians:** Provide personal information through forms, receive communications, and access relevant school information.

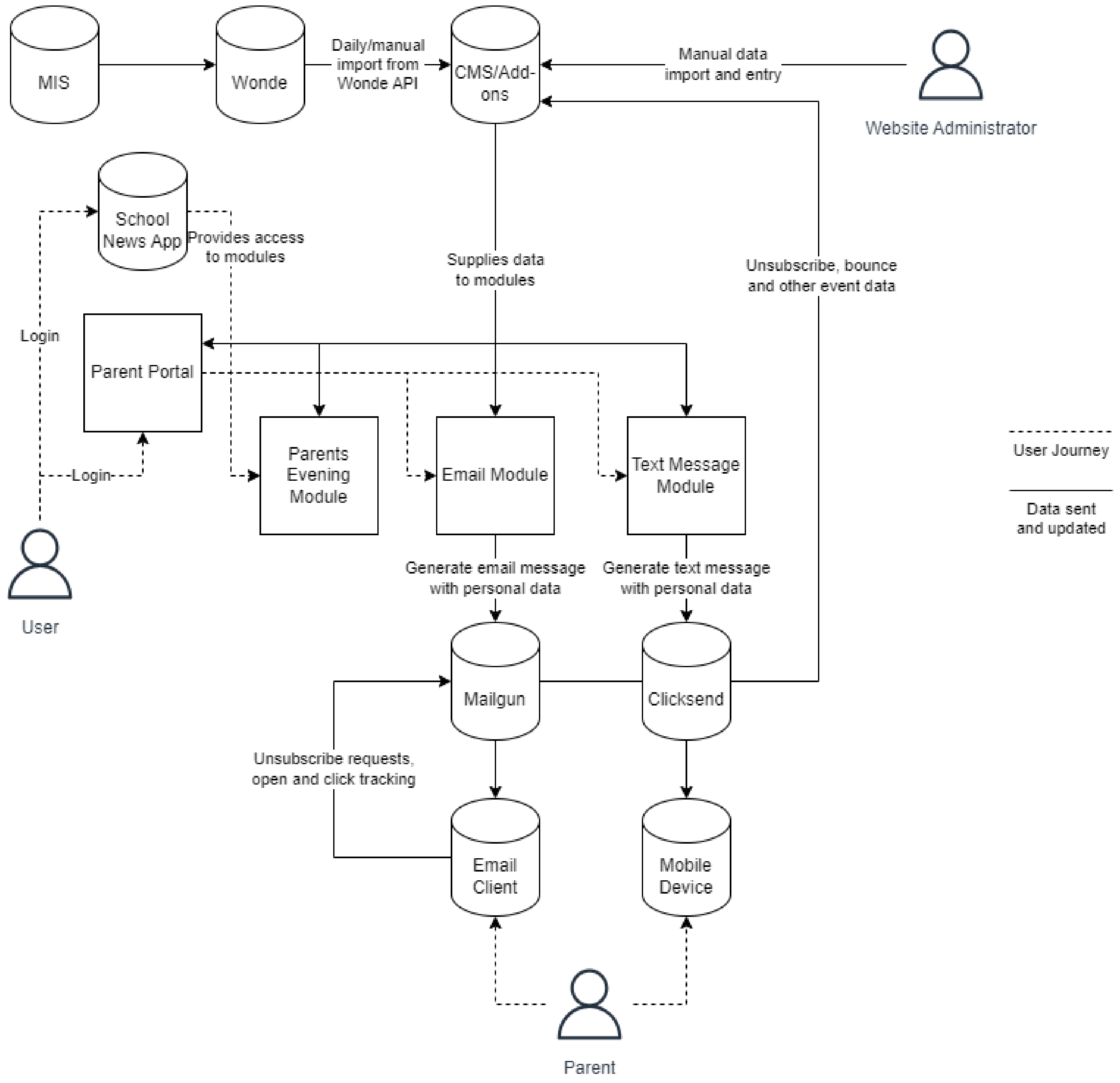
- **Staff:** Manage educational and operational activities, maintain communication with parents and students, and ensure the smooth running of school operations.

- **Website Visitors:** Access public information on the school website.

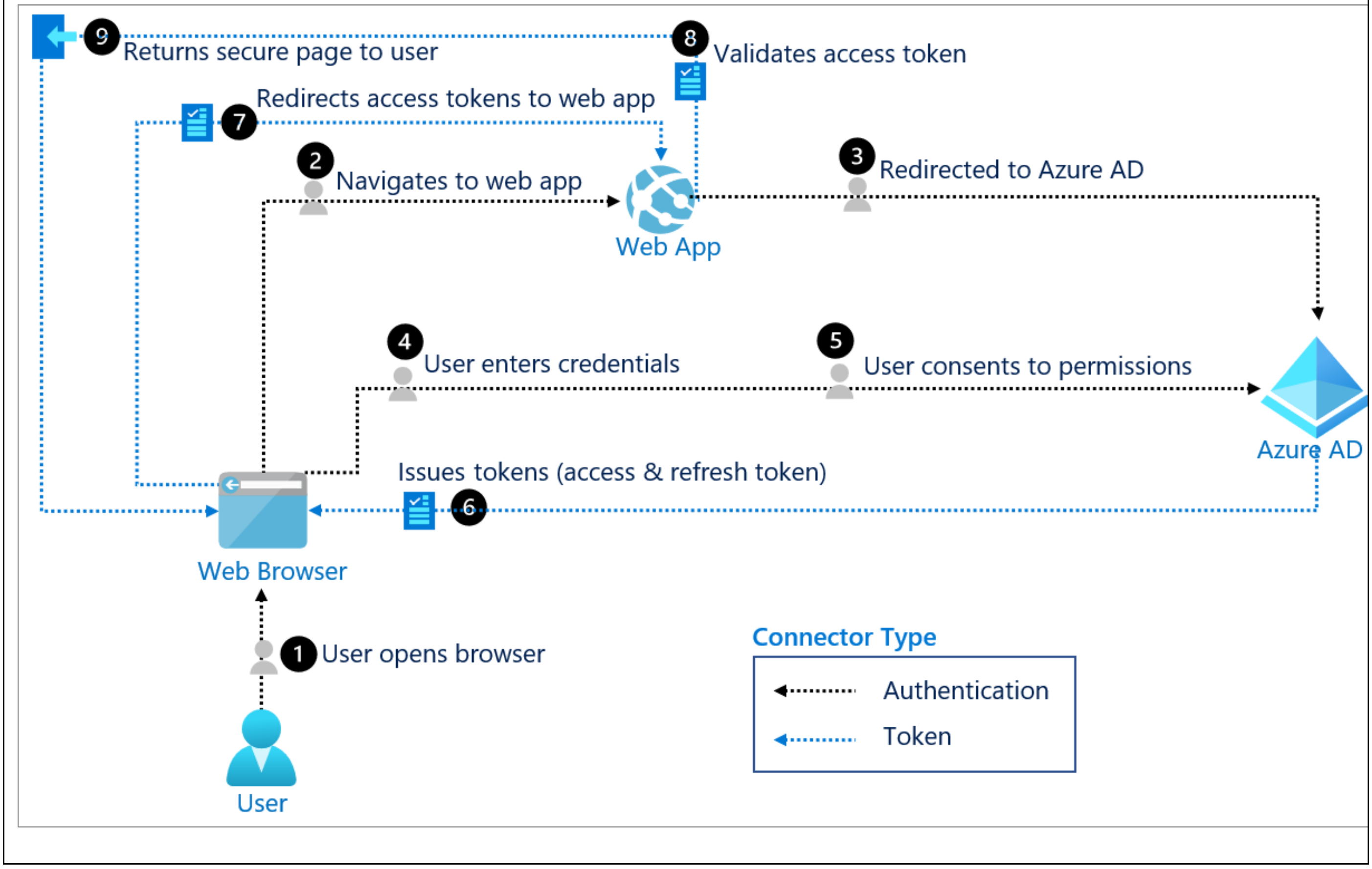
IT Systems

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.

Add-Ons with MIS integration:


MIS
Wonde
Daily/manual import from Wonde API
CMS/Add-ons
Manual data import and entry
Website Administrator
School News App
Provides access to modules
Supplies data to modules
Unsubscribe, bounce and other event data
Login
Parent Portal
Login
Parents Evening Module
Email Module
Text Message Module
User Journey
Data sent and updated
User
Generate email message with personal data
Generate text message with personal data
Mailgun
Clicksend
Unsubscribe requests, open and click tracking
Email Client
Mobile Device
Parent

Single Sign On (SSO):
Microsoft and Google SSO follow the same data flow:


9 Returns secure page to user
8 Validates access token
7 Redirects access tokens to web app
2 Navigates to web app
3 Redirected to Azure AD
Web App
4 User enters credentials
5 User consents to permissions
Azure AD
Issues tokens (access & refresh token)
6
Web Browser
1 User opens browser
User
Connector Type
Authentication
Token

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
Mailgun	Email delivery	EEA	https://www.mailgun.com/gdpr/
ClickSend	Text message delivery	EEA	https://www.clicksend.com/gb/legal/privacy-policy/
Wonde	Sync data from schools MIS to CMS	EEA	https://www.wonde.com/privacy-policy/
AWS	Hosting/Storage	EEA	https://aws.amazon.com/compliance/data-protection/
Twitter	CMS users with permissions can push public facing content.	US	https://x.com/en/privacy
Facebook	CMS users with permissions can push	US	https://www.facebook.com/privacy/policy/

	public facing content.		
Instagram	CMS users with permissions can push public facing content.	US	https://privacycenter.instagram.com/policy

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

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?

Juniper Websites is committed to ensuring personal data collected or created through the CMS 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 access control system restricts access to personal data based on user roles and permissions. Users can only access data necessary for their specific tasks within the CMS.

- **Data Minimisation:** We encourage schools to adopt data minimisation practices. This means collecting and storing only the minimum amount of personal data necessary for the intended purpose (e.g., staff directory, parent portal).

- **Data Retention Policy:** Outlined in Terms of Business.
- **User Training:** Juniper Websites provides regular training to its staff on data protection principles and ensure they understand the importance of using personal data only for authorised purposes.
- **Data Processing Agreements:** Data processing agreements in place with sub-processors.

Additional:

- **School Responsibility:** Schools using the CMS are ultimately responsible for ensuring data is processed in accordance with their agreements and data protection regulations. Juniper provides resources and guidance to support this.

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?

- **Functionality Design:** The CMS functionalities are designed to minimise data collection by default. Schools can choose to add specific data fields only if necessary for their intended purpose (e.g., customising staff directories or forms).
- **Clear Documentation:** We provide clear documentation to schools outlining the types of personal data typically collected through the CMS and its various functionalities. This helps schools make informed choices about data collection practices.
- **Configurable Settings:** The CMS offers configurable settings that allow schools to control the data collected through forms or website content creation. This empowers schools to tailor data collection to their specific needs.

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?

Juniper Websites takes steps to promote data accuracy within the CMS environment. However, the ultimate responsibility for ensuring accurate data lies with the schools using the platform.

Measures by Juniper Websites:

- **Data Validation:** The CMS incorporates data validation functionalities to check for inconsistencies or invalid formats during data entry (e.g., verifying email addresses). If the CMS's data validation functionalities fail to accurately check for inconsistencies or invalid formats during data entry, such as verifying email addresses, it can lead to the storage of incorrect or incomplete data.

- **Data Sync:** For sites that integrate with Wonde to use MIS data in the CMS, we perform daily and manual data synchronisation to ensure information remains up to date. Failure to maintain current parental rights data could lead to unauthorised access, where a parent with a court order may access child data when they shouldn't, or conversely, a parent may be denied access to child data when they should have it.

- **Reminder Feature for Pages and Documents:** The CMS notifies designated users to update documentation as the specified due date approaches. If pages and documents are not up to date, critical documents may remain outdated, leading to potential non-compliance and operational inefficiencies.

- **Security Measures:** Robust security measures help prevent unauthorised data modification, promoting data integrity. Failure to maintain security measures may result in unauthorised access, data modification which would compromise data integrity, potentially lead to breaches and loss of trust.

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?

Media

- Photography (raw): 3 months from the date photography is taken.
- Photography (edited): 1 year from the date photography is taken.

Virtual Tours:

- Raw images: 3 months from the date photography is taken.
- Final tour: For the duration of the contact, or date client requests removal, whichever is longer.

Videography

- Raw footage: 3 months from final approval.
- Edited footage: For the duration of the contract, or date client requests removal, whichever is longer.

Websites

- **Backups kept throughout contract duration:** During the contract period, backups will be maintained. In the event of a client terminating their contract with Juniper, we will preserve a backup for 3 months following the client's request to deactivate the website. Access to the website during this period may result in charges for the duration of access needed. It's important to note that any data considered personal data will not be retained and will be deleted unless otherwise requested at the time-of-service cancellation.

Design files:

- The final file to be retained for 5 years from the date of sign off. All other files to be retained for 6 months from period of design sign off.

Prospectuses:

- Final approved design will be retained for a period of 2 years.

Content (word documents)

- 3 months after the site is live.

Personal data:

- In the instance that the school is no longer a client of the company, a maximum of 5 working days from the date this agreement terminates.

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 Websites takes data security seriously and implements a comprehensive set of measures to ensure the confidentiality, integrity, availability, and restorability of data, data systems, and processes within the CMS environment. Key technical and organisational security controls are outlined below:

- Juniper is migrating from OVH to AWS by Q1 2025, which will enhance infrastructure security.
- AWS services are configured to block all access by default, with Security Groups managing permissions.
- VPN access, encryption at rest is implemented as part of AWS with advanced DDoS protection currently being investigated.
- Access is managed via Microsoft and Google SSO, with Multi-Factor Authentication (MFA) enabled.
- Passwords are salted and hashed; policies enforce strong password hygiene and inactivity alerts.
- Malware protection is optional via AWS, but its implementation is currently being considered; current security uses manual WAF rules (e.g., Vanish).
- Vulnerability scanning is performed regularly but still linked to manual update processes.
- Backups are stored in AWS S3 with 2-hour intervals and multi-period retention (180 days).
- AWS automated patching and peer-reviewed change controls are in place.
- Planned SIEM/SOC monitoring, logging, and periodic penetration testing to support threat detection.
- All personal data is encrypted at rest; no plain text storage is used anywhere in the environment.
- A disaster recovery solution is integrated within the AWS platform.
- Juniper enforces detailed data retention and secure development policies.

Juniper

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

Junipereducation.org